DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

PROYECTO FIN DE CARRERA

DISEÑO DE UNA RED DE TELECOMUNICACIONES EN UN CENTRO DE COWORKING

Ingeniería Técnica de Telecomunicaciones: Sonido e imagen

Julio 2015

Autor: Irene Sánchez Blázquez

Tutor: María Calderón Pastor

Leganés, 15 de Julio de 2015

Título: **DISEÑO DE UNA RED DE TELECOMUNICACIONES EN UN CENTRO DE COWORKING**

Autor: Irene Sánchez Blázquez

Tutor: María Calderón Pastor

EL TRIBUNAL

Presidente: Carlos J. Bernardos Cano

Vocal: Jesús Arias Fisteus

Secretario: Ángel Bravo Santos

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 15 de Julio de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

A mis padres y a mi hermano, por todo su apoyo.
A Miguel, por ayudarme y hacerme más fácil el camino.
A María, porque sin su confianza y ayuda no habría sido posible finalizar este proyecto.

Muchas gracias a todos.

Resumen

El diseño de redes es una práctica necesaria y habitual hoy en día en prácticamente todos los sectores profesionales. Nuestra forma de comunicarnos y de compartir información ha evolucionado a lo largo de los años impulsada por el desarrollo de las nuevas tecnologías dando lugar a una enorme expansión y enriquecimiento de las redes de telecomunicaciones. De dicha expansión y más en concreto de las posibilidades y servicios que una red puede ofrecernos, han surgido nuevos negocios y otros han ampliado sus actividades y mejorado la eficiencia en el desempeño de sus tareas.

El presente proyecto tiene como objetivo el diseño de una red de telecomunicaciones en un centro de coworking. En concreto se llevará a cabo el diseño de la red cableada e inalámbrica, teniendo en cuenta que la red resultante deberá ofrecer un servicio de videoconferencia y un servicio de impresora, fax y escáner. Además, la red a diseñar deberá ser una red segura, por lo que se incluye en el diseño el equipamiento de seguridad necesario para este fin.

La solución técnica se abordará comenzando por la descripción del diseño de la red cableada, incluyendo en el mismo la solución a los servicios de videoconferencia e impresora, fax y escáner, y continuando por el diseño de la red inalámbrica. La descripción de cada uno de estos diseños incluirá la descripción de la arquitectura de red empleada (física y lógica), así como el dimensionamiento del equipamiento necesario para cumplir con este diseño. Por último se detallará la conectividad física de todo el equipamiento de red mediante las tablas de conexiones por dispositivo y el diagrama físico, y se incluirá una planificación de las fases para llevar a cabo el despliegue de la red y el presupuesto económico de toda la solución propuesta.

Palabras Clave: solución técnica, red cableada, red inalámbrica o inalámbrica, servicio de videoconferencia, diseño o arquitectura de red, diagrama físico, planificación despliegue, presupuesto económico.

Abstract

Network design is a necessary and common practice today in almost all occupational sectors. The way we communicate and share information has evolved over the years through the development of new technologies leading to a huge expansion and the enhancement of telecommunications networks. Due to that recent expansion and the new possibilities and services that a network can offer, new businesses have emerged and others have expanded its activities and improved efficiency in the performance of their tasks.

This project aims to design a telecommunications network in a coworking center. In particular it will carry out the design of a wired and wireless network, considering that the resulting network should provide videoconferencing and printer/fax/scanner services. In addition, the network should be secured, so the security devices necessary for this purpose are included in the design.

The technical solution will be defined starting with the design of the wired network, including the solution of the videoconference device and printer, fax and scanner services, and continuing with the design of the wireless network. Each of these designs include the description of the network architecture (physical and logical) as well as the type and number of the devices necessary to meet the requirements. Also the physical connection of network devices will be detailed explaining the connections per device and the physical diagram will be included. Finally the plan to carry out the deployment of the network and the financial budget of the entire solution will be created and added.

Keywords: technical solution, wired network, wireless network, videoconferencing, design and network architecture, physical diagram, deployment planning, financial budget.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

El objetivo del presente documento es desarrollar la memoria del proyecto fin de carrera en el que se ha abordado el problema de diseñar una red de telecomunicaciones. En concreto se contempla como caso de estudio el diseño de una red de telecomunicaciones en un centro de coworking.

1.1 Contexto y Motivación

Hoy en día existen múltiples empresas dentro del sector de las telecomunicaciones que llevan a cabo el diseño y despliegue de redes de diferentes tipos para todo tipo de negocios.

Para desempeñar esta tarea se debe adoptar cierta metodología en la fase inicial, que permita recopilar todos los aspectos importantes que se necesitan tener en cuenta para el diseño de una red. Esto implica el conocimiento del negocio para el que se requiere la red, no sólo a nivel de servicios que pueda necesitar sino también en aspectos relativos al propio negocio, como volumen de usuarios que harán uso de la red, crecimiento en los últimos años, previsiones de crecimiento y/o de ampliación, diversificación de negocio, posibles sinergias…

Según la importancia que tenga la red en el negocio y los servicios que esta ofrezca, estos aspectos tendrán mayor o menor impacto en el diseño de la misma. Debido a que cada vez es más habitual que la red sea el sustento del propio negocio o un medio fundamental para el desarrollo del mismo, todos los cambios previstos que tengan que ver con el negocio deben ser conocidos en la medida de lo posible desde el punto inicial de elaboración del diseño de la red.

1.2 Objetivo

Para el desarrollo del presente proyecto fin de carrera se ha tomado como caso de estudio la elaboración del diseño de una red de telecomunicaciones para un centro de *coworking*.

El objetivo del proyecto es desarrollar el diseño completo de la red incluyendo el diseño de la red cableada y red inalámbrica y de todos los servicios que se exponen como requisitos en el caso de estudio. Además del diseño, se incluye una planificación del despliegue de la red y el presupuesto para la ejecución de toda la solución técnica propuesta.

1.3 Marco regulador y entorno socioeconómico

1.3.1 Marco regulador

En este apartado se analizan las posibles restricciones técnicas o legales que aplican al objetivo del presente proyecto fin de carrera.

El ámbito de las telecomunicaciones en España está regulado por la **Ley 9/2014, de 9 de mayo, de Telecomunicaciones.** En relación al caso particular que se aborda en el desarrollo del presente proyecto no existe ninguna restricción legal o técnica que aplique a dicho caso.

1.3.2 Entorno socioeconómico

En este apartado se analiza cual es el entorno social y económico en el que se enmarca el objetivo del presente proyecto fin de carrera.

La sociedad actual demanda nuevos medios y entornos de desarrollo profesional que no impliquen un desembolso económico elevado. Los centros de coworking son una opción accesible para el desarrollo profesional individual y colectivo en empresas pequeñas, aportando el enriquecimiento de compartir un mismo espacio físico con diferentes profesionales de nuestro mismo sector y sectores diferentes.

Por otro lado, vivimos bajo un crecimiento constante del desarrollo de las redes de telecomunicaciones y los servicios que estas pueden ofrecernos. Este crecimiento nos empuja a cambiar nuestra forma de interactuar y acceder a la información en todos los ámbitos. En el ámbito profesional, los beneficios de este desarrollo son conocidos cada vez más tanto por las empresas dedicadas al diseño y despliegue de redes, como por cualquier cliente de dichas

empresas que conoce cada vez con más detalle los beneficios operativos y económicos que un diseño adecuado de su red puede ocasionarle para su negocio.

1.4 Estructura del documento

El documento se estructura en los siguientes apartados:

- **Estado del Arte:** En este capítulo se resumen los fundamentos teóricos más importantes de los que se hace uso en el desarrollo del presente proyecto. Se incluyen los siguientes apartados:
    - Redes virtuales o VLANs: 802.1Q
    - Direccionamiento IP
    - Network Address Translation (NAT)
    - Seguridad en las redes: firewalls
    - Estudio de cobertura inalámbrica
    - Sistemas de videoconferencia

- **Caso de Estudio:** Este bloque recoge la información relativa a la definición del caso de estudio que se pretende resolver; esta información se completa con el Anexo III: Planos de Planta incluido al final del documento.

- **Solución Técnica:** Se trata del bloque principal del documento, en el que se incluye el desarrollo del diseño de la red de telecomunicaciones objeto del presente proyecto fin de carrera. La solución técnica se aborda atendiendo a los siguientes apartados:
    - Planteamiento inicial de diseño
    - Red cableada
    - Red inalámbrica
    - Ampliación de detalles de diseño
    - Diseño físico
    - Servicios de instalación (planificación y presupuesto)

- **Conclusiones:** Se resumen las conclusiones más importantes del proyecto.
- **Referencias:** Se exponen las referencias utilizadas en la elaboración del proyecto.
- **Anexo I: Equipamiento.** Este anexo recoge el detalle del equipamiento que se ha considerado para la elaboración de la solución técnica.
- **Anexo II: Presupuesto del proyecto fin de carrera:** Este anexo recoge el presupuesto económico resultante del desarrollo del presente proyecto fin de carrera.
- **Anexo III: Planos de planta:** Se incluyen los planos de planta del centro de coworking definido en el caso de estudio.

Capítulo 2

Estado del arte

En el presente capítulo se pretende ofrecer una recopilación de los conceptos teóricos más importantes aplicados en el desarrollo del proyecto.

2.1 Redes Virtuales o VLANs

Una red virtual o VLAN (Virtual Local Area Network), es una red lógica independiente que puede coexistir con otras redes lógicas dentro de un mismo switch o una misma red física. El uso de redes VLAN permite limitar los dominios de difusión, facilitar la administración y gestión de la red al separar la misma en segmentos lógicos en función del tipo de tráfico que se transmite en cada uno de ellos.

El estándar que define y regula la utilización de VLANs en una red Ethernet es el estándar **IEEE 802.1Q**. Este estándar se basa en un sistema de etiquetado para las tramas Ethernet que consiste en añadir cuatro bytes al encabezado Ethernet original destinados a indicar principalmente el identificador de la VLAN a la que pertenece la trama y un campo de prioridad que indica la prioridad de los datos que contiene la misma.

Existen diferentes tipos de VLAN en función del parámetro de configuración que las define, las más habituales son las que se definen en el puerto del switch, son también conocidas como VLAN de nivel 1 o VLAN basadas en puerto. Cuando un dispositivo se conecta a un puerto de un switch que tiene configurada una VLAN automáticamente comienza a pertenecer a la VLAN a la que ha sido asignado el puerto.

Otros tipos de VLAN en función del nivel en el que operen son:

- VLAN de nivel 2 (o VLAN por dirección MAC): son aquellas que se definen según la dirección MAC del dispositivo. Se trata de un tipo de VLAN más flexible que la

VLAN de nivel 1 o basada en puerto, ya que la pertenencia a una VLAN determinada es independiente de la ubicación del dispositivo.

- VLAN de nivel 3, podemos distinguir entre dos tipos:
  - VLAN basada en la dirección de red. Se trata de un tipo de VLAN que se define en función de la dirección IP origen de los paquetes. Es un tipo de VLAN flexible pero que requiere del análisis de los paquetes.
  - VLAN basada en protocolo. Son aquellas VLAN que se definen en función de un tipo de protocolo, permitiendo agrupar todos los equipos que utilizan el mismo protocolo en una misma red lógica.

El tipo de VLAN de nivel 1 o basada en puerto es una VLAN estática ya que la pertenencia de un dispositivo a este tipo de VLAN depende directamente de la configuración del puerto al que se conecta físicamente el dispositivo. En contraposición se encuentran las VLAN dinámicas, las cuales se definen mediante software específico que permite asignar dinámicamente los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo.

2.2 Direccionamiento IP

La metodología actual para la asignación de direcciones IP es conocida como CIDR (Classless Inter-Domain Routing) y supone una mejora de la anterior metodología basada en la asignación de clases de direcciones (clase A, B o C) cada una de ellas con un prefijo de red fijo (8, 16 o 24 bits).

La metodología CIDR sustituye a la anterior asignación de clases de direcciones con prefijos de red fijos y permite la asignación de direcciones con prefijos de red de tamaño variable, haciendo un uso más eficiente de las direcciones IP ajustado a las necesidades concretas de la red, esta técnica se conoce como VLSM (Variable Length Subnet Mask).

Podemos distinguir entre dos tipos de direcciones IP:

- ***Direcciones IP Privadas***: Son las direcciones IP asignadas a los dispositivos de red dentro de una red local (red LAN) que no tienen acceso directo a Internet. Los rangos reservados para el direccionamiento privado son:
  - 10.0.0.0 /8
  - 172.16.0.0 /12
  - 192.168.0.0 /16

- ***Direcciones IP Públicas***: Son las direcciones IP asignadas a los dispositivos de red que tienen conectividad con Internet y que por lo tanto deben ser únicas en toda la red de internet.

2.3 Network Address Translation (NAT)

Network Address Translation o NAT es un mecanismo que emplean los routers para traducir direcciones IP privadas o internas a direcciones IP externas o públicas.

De esta forma, una red local utiliza un rango de direcciones IP privadas y una única dirección IP pública para la salida a Internet. El equipo de router o nivel 3 que proporciona la salida a Internet es el encargado de desarrollar el mecanismo NAT para la traducción de direcciones privadas a públicas. Existen varios tipos de funcionamiento del mecanismo NAT:

- ***NAT estático***: Consiste en vincular una dirección IP privada con una dirección IP pública, siendo esta dirección IP pública siempre la misma. Esto permite a un host de una red privada tener una dirección IP privada pero a la vez ser visible en Internet.
- ***NAT Dinámico***: En este caso el router dispone de una tabla de direcciones IP públicas de manera que cuando una dirección IP privada necesite acceder a internet el router eligirá una dirección pública de la tabla que no esté siendo usada por ninguna otra dirección privada. Este tipo de mecanismo NAT proporciona una mayor seguridad en la red, dificultando que un host externo ingrese en la red al ir cambiando las direcciones públicas.
- ***Sobrecarga (Overload)***: Es el tipo más utilizado ya que permite mapear múltiples direcciones IP privadas a través de una única dirección IP pública, mediante la asignación de un número de puerto de conexión.

2.4 Alta disponibilidad: modos activo-activo y activo-pasivo

Hacemos uso del término alta disponibilidad en redes de telecomunicaciones para referirnos a todos aquellos diseños o arquitecturas de red que garantizan la continuidad del servicio mediante la aplicación de esquemas de redundancia y mecanismos de protección contra fallos.

Los esquemas de redundancia más comunes se basan en replicar aquellos componentes hardware de nuestra red más críticos como por ejemplo las fuentes de alimentación. Otras

medidas de redundancia más avanzadas se basan en configuraciones de cluster de dos o más equipos en alta disponibilidad.

Un **cluster en alta disponibilidad** es un conjunto de dos o más equipos de red conectados entre sí y configurados de tal forma que si se produce un fallo en alguno de ellos, el resto de equipos que forman el cluster pueden continuar ejecutando sus funciones sin que se produzca ninguna interrupción en el servicio.

Las configuraciones más comunes de alta disponibilidad son la configuración en activo-activo y la configuración en activo-pasivo.

- **Alta disponibilidad: activo-activo.**

La configuración de alta disponibilidad en activo-activo se caracteriza porque todos los equipos que forman el cluster están accesibles y operativos simultáneamente. Es decir, todos los equipos que forman el cluster poseen la misma configuración física y lógica con respecto al resto de elementos de la red, de tal forma que si se produce un fallo en cualquiera de los equipos que forman el cluster, el resto de equipos del cluster mantienen la continuidad del servicio.

La principal ventaja de este tipo de configuración es que todos los equipos que forman el cluster están activos simultáneamente mejorando además de la alta disponibilidad, el rendimiento del servicio. Sin embargo, si se produce un fallo en alguno de los equipos, su carga de trabajo pasa a repartirse entre el resto, lo que produce una degradación del rendimiento del servicio respecto a la configuración inicial.

- **Alta disponibilidad: activo-pasivo**

La configuración de alta disponibilidad en activo-pasivo, consiste en que sólo uno de los equipos que forman el cluster está activo, mientras que el resto tienen la misma configuración y capacidad de dar el servicio pero sólo pasan a estado activo en caso de fallo del equipo que está activo inicialmente.

La principal ventaja de esta configuración es que no se produce degradación en el rendimiento del servicio en caso de que se produzca un fallo. Sin embargo, es una configuración menos eficiente, ya que mientras que no se produce ningún fallo, los equipos que están en modo pasivo no son utilizados.

2.5 Seguridad en las redes

Consideramos que una red es segura, si logra reducir todas sus vulnerabilidades.

Según la normativo ISO-27001 en el contexto de la informática se considera **vulnerabilidad** a cualquier flaqueza que pueda ser aprovechada para violar un sistema o la información que este contiene. Las violaciones de seguridad se pueden clasificar como **amenazas**, siendo las siguientes las más destacables:

- Destrucción de la información.
- Modificación de la información.
- Robo, pérdida de la información o recursos.
- Interrupción del servicio.

Cuando una amenaza se lleva a cabo la consideramos un **ataque**. Podemos distinguir entre los siguientes tipos de ataques:

- Ataques a la confidencialidad.
- Ataques a la autenticidad.
- Ataques a la disponibilidad.
- Ataques de modificación y daño.

A la posibilidad de que ocurra un ataque la consideramos **riesgo**. Para poder dotar de seguridad a una red es recomendable realizar en primer lugar un análisis del riesgo. Una metodología habitual para el análisis del riesgo, consiste en evaluar el coste total necesario para implantar las medidas de prevención, y comprobar si es menor al coste que supondría perder el activo que intentamos proteger, en caso afirmativo debemos aplicar una medida de prevención de ataques a nuestra red.

Las acciones más recomendables para elaborar medidas de prevención frente ataques consisten en la elaboración del diseño lógico de nuestra red planificando la seguridad (mediante la separación en subredes, tipos de tráfico, etc), y la inclusión de dispositivos de control como los **firewalls**.

2.5.1 Firewalls

El firewall es un dispositivo de red que nos permite aplicar políticas de control y filtrado de tráfico entre varias redes o subredes.

Se trata del elemento central del diseño lógico de nuestra red, ya que para que su uso sea efectivo debe ser atravesado por todo el tráfico que se transmite de una subred a otra. Desde el punto de vista funcional existen dos tipos de firewalls:

- ***Firewalls de filtrado de paquetes:*** Se trata de aquellos firewalls que analizan el contenido de los paquetes que los atraviesan y realizan filtrado de los mismos en función de este contenido, existen dos tipos de filtrado:
  - ***Filtrado de paquetes estático:*** consiste en la inspección individual de cada paquete analizando parámetros como la dirección origen y dirección destino, y aplicando reglas bajo las cuales se permite el envío del paquete o se procede al descarte del mismo.
  - ***Filtrado de paquetes dinámico (verificación de estado):*** consiste en mantener un registro del estado de la comunicación y analizar si la secuencia de paquetes transmitidos se corresponde al estado actual de la comunicación.
- ***Proxy firewalls:*** Se trata de aquellos firewalls que evalúan los paquetes a nivel aplicación permitiendo el filtrado de contenidos y comandos de aplicación.

En el mercado existe una gran variedad de fabricantes de firewalls cada uno de los cuales emplea una arquitectura determinada, podemos distinguir entre los siguientes dos tipos de arquitectura:

- ***Arquitectura con gestora integrada en el dispositivo:*** Se trata de aquellos firewall en los que la parte dedicada a la gestión del mismo está integrada dentro del propio dispositivo de firewall. En este caso, sólo disponemos de un equipo físico, al cual nos conectamos para gestionarlo o configurarlo, crear reglas, aplicar filtros, etc.

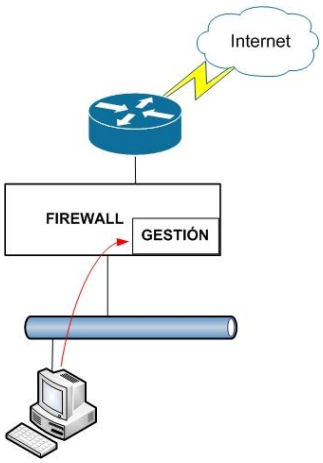


Figura 1. Conectividad con gestora integrada en el firewall

- ***Arquitectura con gestora independiente:*** Se trata de aquellos firewall en los que la parte del dispositivo encargada de la gestión del mismo se encuentra físicamente separada en un dispositivo aislado denominado gestora. La gestora puede estar conectada en cualquier punto de nuestra red siempre y cuando exista comunicación entre ella y el firewall. En esta arquitectura, para gestionar el firewall debemos conectarnos a la gestora la cual enviará la información al firewall para su gestión.

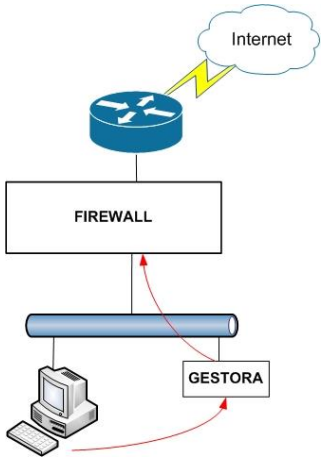


Figura 2. Conectividad con gestora independiente

La arquitectura con gestora independiente suele emplearse en redes con más de dos firewalls en las que la gestión centralizada de todos los firewalls mediante una única gestora externa supone una gran ventaja en cuanto a facilidad de administración. En redes más pequeñas, con solo una pareja de firewall es más habitual una arquitectura con la gestora integrada en cada dispositivo por ahorro de costes, al no ser tan problemática la gestión de cada firewall de forma independiente.

◆ *Cluster de dos firewalls en alta disponibilidad, modo activo-pasivo*

El firewall es un elemento crítico para el mantenimiento de la seguridad en nuestra red, es por ello que una configuración recomendable consiste en configurar un cluster de dos firewalls de **alta disponibilidad** en **modo activo-pasivo**. Las condiciones para establecer un cluster de firewalls en alta disponibilidad es que los dos dispositivos de firewall que formen el cluster sean iguales a nivel hardware y software.

El primer paso para la configuración del cluster es configurar la gestora del primero de los firewall que será el firewall principal. Se dan de alta en la gestora los firewalls que se van a gestionar desde la misma indicando que se trata de un cluster; estos firewalls serán el mismo firewall que contiene la gestora que estamos configurando, y el segundo firewall que forma

parte del cluster. Una vez que han sido dados de alta todos los firewalls en la gestora y se han declarado como cluster, a nivel lógico es como si tuviéramos un único firewall.

En el momento en el que se dan de alta en la gestora todos los firewalls que forman el cluster, ésta adquiere la topología de todos los firewalls. Con esta información, la gestora establece su tabla de topología de cluster, la cual contiene para cada una de las interfaces o subinterfaces de cada firewall que ha detectado, la dirección IP y máscara que tienen asignada.

Además, para cada interfaz o subinterfaz del firewall principal, se debe completar un campo dentro de la tabla de topología de cluster denominado **VIP** o **Virtual IP**, que será una dirección IP que pertenezca a la misma red de la interfaz o subinterfaz correspondiente. Estas direcciones VIP serán las que se configurarán como puerta de enlace en los dispositivos que estén conectados a cada interfaz o subinterfaz de los firewall. Sólo se configura una dirección VIP para cada interfaz o subinterfaz del firewall principal o activo.

Los dos firewalls del cluster deben disponer de una **interfaz de sincronización**. Esta interfaz está destinada a la comunicación entre los dos firewalls que forman el cluster y aunque está registrada dentro de la tabla de topología del cluster de la gestora, no tiene configurada ninguna dirección VIP.

A media que se produce el flujo del tráfico en la red, el firewall principal recibe y almacena una serie de información (tablas NAT, tablas de conexiones, etc), toda esta información la comparte de forma automática con el firewall secundario a través de la interfaz de sincronización. Además de esta información, los dos firewalls que forman el cluster están intercambiando constantemente información sobre su estado a través de esta interfaz. De esta forma, el firewall secundario puede detectar cuando el firewall principal no está disponible, y es en ese momento cuando el firewall secundario adquiere las direcciones VIP que estaban asignadas al firewall principal dentro de la tabla de topología del cluster y pasa a actuar como firewall principal o activo.

Los motivos principales por los cuales el firewall secundario pasa a adoptar el rol de firewall activo son:

- Si el firewall principal le informa de que una de sus interfaces está caída.
- Si el firewall principal se apaga y no responde.
- Si el firewall principal tiene cualquier tipo de error de sistema operativo y no responde.

Una vez que se solventa el fallo, existen diferentes funcionamientos dependiendo del fabricante, algunos modelos funcionan restableciendo los roles iniciales de firewall principal y secundario una vez que se ha solventado el fallo, otros mantienen los roles que se han adquirido cuando se ha producido el fallo y no los restablecen a la configuración inicial hasta que no se vuelven a aplicar nuevas políticas o reglas desde la gestora.

2.6 Estudio de cobertura inalámbrica

Para el diseño de cualquier red inalámbrica es necesario realizar un estudio de cobertura previo sobre la zona que nos ayude a determinar el número de puntos de acceso que necesitamos así como la ubicación física de los mismos de tal manera que podamos garantizar un nivel de cobertura óptimo en toda la superficie.

Existen multitud de herramientas software en el mercado para la realización de Estudios de Cobertura Inalámbrica, para el desarrollo del presente proyecto se hará uso del software *Ekahau Site Survey 6.0*

Los materiales necesarios para la realización del Estudio de Cobertura son:

- Software *Ekahau Site Survey 6.0*
- PC portátil con adaptador inalámbrico Ekahau
- Punto de acceso inalámbrico (modelo previamente seleccionado según el tipo de entorno con el que vamos a trabajar (oficina, fábrica, exterior… etc))
- Mástil para la ubicación del Punto de acceso en altura

Figura 3. Materiales estudio de cobertura

El estudio de cobertura consiste en ubicar el punto de acceso con ayuda del mástil en un punto determinado de la superficie e ir tomando mediciones desde el resto de zonas mediante la antena inalámbrica instalada en el PC con el software Ekahau Site Survey. De esta forma, para cada ubicación del punto de acceso, se debe recorrer toda la superficie tomando mediciones que se registran en el software Ekahau Site Survey y dan como resultado un mapa

de cobertura en el que se muestra la intensidad de la señal recibida (en dBm) en cada punto de la superficie.

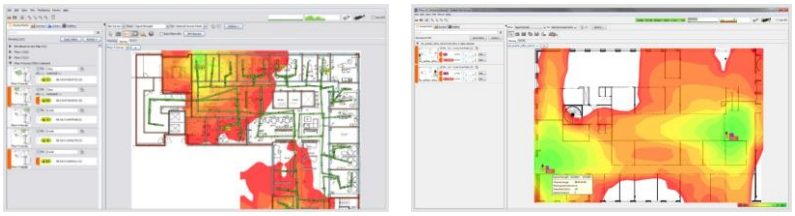


Figura 4. Ejemplo mapas de cobertura Ekahau Site Survey

La unidad de potencia utilizada para expresar la intensidad de la señal recibida es el dBm (dBmW o decibelio-milivatio), aunque también se suele denotar la intensidad de la señal recibida mediante el *Indicador de fuerza de la señal recibida* o RSSI en sus siglas en inglés (*Received Signal Strength Indicator*). En una escala de 0 a -80 dBm podemos considerar los siguientes escenarios:

- 0 dBm señal ideal, difícil de lograr en la práctica.
- -40 a -60 dBm: señal idónea con tasas de transferencia estables.
- -60 dBm: enlace bueno
- -70 dBm: enlace normal-bajo
- -80 dBm: es la señal mínima aceptable para establecer la conexión

Para que el Estudio de Cobertura tenga mejores resultados debe realizarse en las condiciones de uso habitual de la superficie (mobiliario, materiales, personas, etc.) con el fin de tener en cuenta todos los factores que puedan afectar a la propagación de la señal.

Antes de comenzar a realizar el estudio, es necesario cargar el plano de la superficie que vamos a recorrer en el software Ekahau Site Survey y realizar algunas configuraciones sobre los requisitos de la red Inalámbrica que pretendemos diseñar. Por ejemplo, en relación a la cobertura: área de cobertura (delimitar el área exacta del plano que queremos cubrir), banda de frecuencia sobre las que vamos a emitir (2,4GHz o 5GHz) o tipo de tráfico: datos, video, voz sobre IP, etc; En relación a la capacidad: densidad de clientes Wi-Fi (más de un cliente Wi-Fi por usuario) o tipo de aplicaciones según tipo de cliente Wi-Fi (HD video, e-mail, skype… etc.)

Además del mapa de cobertura o mapa de potencia de la señal, Ekahau Site Survey permite extraer otras mediciones como la relación señal a ruido o el nivel de salud de la red (en función del cumplimiento de los requisitos previamente configurados).

Es recomendable realizar una planificación previa del Estudio de Cobertura, para ello el software Ekahau Site Survey permite realizar una simulación sobre plano sin necesidad de realizar un estudio presencial. Esta simulación consiste en cargar el plano de la superficie y marcar sobre el mismo los materiales de paredes, suelos, puertas y demás superficies que existan, a continuación se seleccionan e incluyen sobre el plano los puntos de acceso indicando la banda de frecuencia en la que queremos que radien y se obtiene el mapa de cobertura resultante sobre toda la superficie.

2.7 Sistemas de Videoconferencia

Un sistema de videoconferencia se define como un conjunto de dispositivos hardware y software que mediante el desarrollo de una serie de tecnologías de telecomunicación permiten interactuar a personas situadas en dos o más ubicaciones alejadas entre sí mediante transmisiones de audio y video bidireccionales concurrentes.

La tecnología básica que emplea un sistema de videoconferencia consiste en la compresión digital del flujo de audio y video en tiempo real. El hardware y/o software que realiza esta compresión es el **codec**, también conocido como **codificador-decodificador**.

Los componentes básicos de un sistema de videoconferencia son:

- **Entrada de video** o cámara
- **Salida de video** (monitor, proyector o pantalla)
- **Entrada de audio** o micrófono
- **Salida de audio** (altavoz o auriculares)
- **Transferencia de datos**, a través de una red LAN y/o internet

En el mercado existe una gran variedad de sistemas de videoconferencia que podemos clasificar en tres grandes grupos:

- ***Equipos de terminal de usuario:*** Se trata de pequeños dispositivos que disponen de una cámara y una pantalla pequeña con micrófono y altavoces integrados, que están pensados para el uso individual y generalmente se ubican en un puesto de trabajo o escritorio.

- ***Equipos para salas de videoconferencia***: Se trata de dispositivos más grandes pensados para ubicarse en salas medianas o grandes y poder realizar videoconferencias en las que en un mismo extremo puedan participar varias personas ubicadas físicamente en la misma sala.

- ***Salas de videoconferencia inmersiva***: En este caso la totalidad de la sala forma el sistema de videoconferencia, desde las paredes, el mobiliario, las pantallas, los micrófonos, etc. Se trata de sistemas que ofrecen una experiencia más completa, real e interactiva a todos los participantes.

Figura 5. Sistemas de videoconferencia

Según el número de sedes y la cantidad de participantes que intervienen en una videoconferencia, estás pueden ser punto a punto (sólo intervienen dos sedes), o multipunto (intervienen más de dos sedes).

Las videoconferencias multipunto necesitan de un dispositivo adicional denominado **Unidad de Control Multipunto (MCU)** que se encarga de conectar a todas las sedes que intervienen en la videoconferencia y distribuir la señal entre las mismas. Hoy en día existen codecs que tienen la funcionalidad de MCU para un número limitado de sedes.

Capítulo 3

Caso de estudio

El caso de estudio que se define para el desarrollo del presente proyecto consiste en el diseño de una red de telecomunicaciones para un centro de coworking.

Los centros de coworking surgen de un nuevo concepto de trabajo colaborativo enfocado principalmente a profesionales que no disponen de oficina física propia pero que desean hacer uso de todos los servicios característicos de dicho espacio. Se trata por lo tanto de oficinas de alquiler que albergan profesionales heterogéneos fomentando así el enriquecimiento profesional y el posible desarrollo de proyectos de forma conjunta.

Algunos de los servicios que ofrecen este tipo de centros son el acceso a internet mediante cable e inalámbrico, el uso de impresora, fax y escáner, salas de videoconferencia, salas de reuniones, salas de formación, despachos, zonas de uso común y descanso, servicio de recepción y almacenaje.

Para el desarrollo del presente proyecto se considera el caso de estudio de un centro de coworking ubicado en un edificio de cinco plantas con las dimensiones y volumen de puestos de trabajo, iniciales y futuros, que se detallan en la *Tabla 3*.

Plantas	Superficie	Nº de puestos de trabajo iniciales	Crecimiento estimado del nº de puestos de trabajo
Planta 0	1105 m^2	154	2 %
Planta 1	1105 m^2	169	1 %
Planta 2	1105 m^2	186	0 %
Planta 3	1105 m^2	186	0 %
Planta 4	1105 m^2	118	3 %
TOTAL	**5525 m^2**	**813**	-

Tabla 1. Características del centro de coworking: dimensiones y número de puestos de trabajo

Los servicios particulares que ofrece el centro de coworking de nuestro caso de estudio son los siguientes:

- **Red cableada** para todos los puestos de trabajo.
- **Red WiFi para usuarios del centro y red WiFi para invitados.**
- **Conexión a Internet.**
- **Servicio de videoconferencia** mediante dos equipos de videoconferencia situados en las plantas 0 y 1, con la posibilidad de realizar videoconferencias con sedes externas hasta un límite de cuatro ubicaciones simultáneas.
- **Servicio de impresora, fax y escáner,** disponiendo de un equipo multifunción en cada una de las plantas que permita estas tres funciones.

Otros servicios ofrecidos por el centro son:

- **Salas de reuniones**, con un total de 2 salas.
- **Despachos privados**, con un total de 25 despachos.
- **Zonas de trabajo abiertas o diáfanas**, con un total de 16 zonas.
- **Zona de descanso exterior**.
- **Cocina.**
- **Recepción.**

En el Anexo II se incluyen los planos de todas las plantas del centro de coworking, así como el detalle de los servicios y características particulares de cada una de ellas.

Además de todos estos servicios, el centro de coworking debe ofrecer una red de telecomunicaciones que cumpla las siguientes características:

- **Seguridad:** La red a diseñar debe disponer de equipos de seguridad como firewalls que controlen el tráfico que circule por la red mediante la aplicación de políticas de filtrado y mecanismos de seguridad.
- **Redundancia:** La red a diseñar debe disponer de mecanismos de redundancia que garanticen una alta disponibilidad del servicio.

El alcance de la solución al presente caso de estudio debe cubrir todos los requisitos mencionados en este apartado. Queda fuera de este alcance la definición del cableado vertical y horizontal de la red de telecomunicaciones.

Capítulo 4

Solución técnica

Según los requisitos definidos en el capítulo 3, se ha diseñado una solución técnica que se presenta de acuerdo a los siguientes apartados:

1. **Planteamiento inicial de diseño:** En primer lugar, definimos en base a los requisitos del capítulo 3, el diseño general de nuestra red que vamos a considerar como punto de partida y que desarrollaremos de manera más detallada a lo largo de los apartados siguientes.
    a. **Definición de VLANs**. El primer aspecto que definiremos como parte de nuestro diseño serán las distintas VLANs o subredes en las que vamos a dividir nuestra red.

2. **Red cableada:** En este apartado abordaremos el diseño de la solución técnica para la red cableada; para ello comenzaremos por la definición del diseño o arquitectura de red elegida y continuaremos por el dimensionamiento del equipamiento de red necesario para cumplir con este diseño. Se incluirá también la solución a los servicios de videoconferencia y servicio multifunción (impresora, fax y escáner)

    a. **Diseño o arquitectura de red.** Dentro de este apartado se desarrolla la arquitectura de red elegida para la red cableada, la cual será una arquitectura basada en capas: con una capa de acceso y una capa de distribución/core.
    b. **Equipamiento.** Para cada una de las capas de la arquitectura de red definida en el apartado anterior, se desarrolla el equipamiento de red necesario.

3. **Red inalámbrica:** En este apartado se desarrolla el diseño de la solución técnica para la red inalámbrica; para ello al igual que en apartado anterior, comenzaremos definiendo el diseño o arquitectura de red empleada y continuaremos por el dimensionamiento del equipamiento de red necesario para cumplir con este diseño. Para el dimensionamiento

del equipamiento se realizará la simulación de un estudio de cobertura mediante el software *Ekahau Site Survey*.

   a. **Diseño o arquitectura de red.** Dentro de este apartado se define el diseño o arquitectura de red empleada para la red inalámbrica, la cual consistirá en una arquitectura centralizada con varios puntos de acceso que serán gestionados de forma centralizada por un controlador redundado.
   b. **Equipamiento (simulación estudio de cobertura)** Mediante la realización de la simulación de un estudio de cobertura se define el equipamiento necesario para cumplir con el diseño definido en el apartado anterior.

4. **Ampliación de detalles de diseño:** Una vez que se ha desarrollado de forma más concreta el diseño o arquitectura de red empleada para la red cableada y la red inalámbrica; en este apartado se terminan de definir los detalles relativos al diseño de nuestra red. En concreto se desarrollan los siguientes apartados:
   a. **Diagrama lógico.** Se representa de forma gráfica el diseño o la arquitectura lógica completa de nuestra red.
   b. **Plan de direccionamiento IP.** Se realiza el plan de direccionamiento IP para la asignación de las direcciones IP de cada subred.

5. **Diseño físico:** En este apartado se agrupan todos los detalles de la conectividad física entre todos los equipos que forman nuestra red y que se han ido definiendo en los apartados anteriores, mediante los siguientes apartados:
   a. **Tablas de conexiones por dispositivo:** Se desarrollan las tablas de conexiones de todos los dispositivos de red, indicando en cada una de ellas el detalle de todas las conexiones (interfaz, velocidad, medio) que tiene cada dispositivo con el resto.
   b. **Diagrama físico:** Se trata de una representación gráfica de las conexiones físicas de todos los equipos que forman nuestra red.

4.1 Planteamiento inicial de diseño

Según los requisitos que se exponen en el capítulo 3, podemos plantear el diseño inicial de nuestra red considerando que ésta estará compuesta a grandes rasgos por una infraestructura de *red cableada* y una infraestructura de *red inalámbrica.*

- La **red cableada** estará formada por varios equipos de red como switches, routers y firewalls, que se conectarán entre sí según una arquitectura de red determinada que se definirá en los apartados siguientes. El objetivo de la red cableada será dar conectividad por cable a todos los terminales de usuarios del centro y proporcionarles acceso a varios

servicios como son el servicio de videoconferencia, el servicio de impresora, fax y escáner, y el servicio de conexión a internet. Por lo tanto, la red cableada albergará fundamentalmente el **tráfico de los usuarios cableados.**

- La **red inalámbrica** estará formada por puntos de acceso y controladores encargados de la gestión de los puntos de acceso que se conectarán a equipos de la red cableada, según una arquitectura determinada que se definirá en los apartados siguientes. El objetivo de la red inalámbrica será proporcionar conectividad inalámbrica a todos los usuarios del centro e invitados. Por lo tanto, dentro de la red inalámbrica podremos distinguir entre los siguientes tipos de tráfico:
  - **Tráfico de dispositivos WiFi**, o tráfico que intercambiarán entre sí los equipos que forman la arquitectura de la red inalámbrica; es decir, los puntos de acceso y los controladores encargados de la gestión de los puntos de acceso.
  - **Tráfico de usuarios WiFi**, o tráfico que generarán los usuarios del centro que se conecten a la red WiFi.
  - **Tráfico de invitados WiFi**, o tráfico que generarán los invitados que se conecten a la red WiFi.

Por otro lado, sabemos que todos los equipos de red disponen al menos de una dirección IP para su gestión de forma remota. Por este motivo, es importante que nuestra red contemple una **red de gestión**, que albergará todo el **tráfico de gestión** de los diferentes dispositivos o equipos de red.

Además de las redes definidas hasta el momento, también nos interesa separar en redes independientes el tráfico de salida a internet, así como el tráfico que será generado por el equipamiento de videoconferencia, y por los equipos multifunción (impresora, fax y escáner). Es por ello que definiremos también una **red de tránsito internet**, una **red de videoconferencia** y una **red de equipos multifunción**.

4.1.1 Definición de VLANs

El primer paso en la elaboración del diseño de nuestra red consiste en establecer la división de nuestra red física en varias redes lógicas o VLANs (Virtual LANs).

El criterio para la definición de VLANs consiste en considerar los diferentes tipos de tráfico que circularán por la red en función de los servicios que queremos cubrir y separar cada tipo de tráfico en una subred o VLAN diferente. La definición de VLANs tiene los siguientes objetivos:

- **Facilitar la aplicación de políticas de seguridad particulares para cada tipo de tráfico**. Al separar cada tipo de tráfico en una VLAN diferente, podemos aplicar reglas de filtrado o políticas de control en los firewalls particulares para cada VLAN y por lo tanto para cada tipo de tráfico.
- **Mejorar la administración y el control sobre la red.** La separación de una red en varias redes lógicas o VLANs permite que la configuración y administración de la red sea más rápida y sencilla.

Según estos objetivos y basándonos en el planteamiento inicial de diseño que se desarrollo en el apartado anterior podemos considerar que nuestra red albergará los siguientes tipos de tráfico:

- Tráfico de usuarios cableados
- Tráfico de dispositivos WiFi
- Tráfico de usuarios WiFi
- Tráfico de invitados WiFi
- Tráfico de gestión
- Tráfico de tránsito internet
- Tráfico de videoconferencia
- Tráfico de equipos multifunción

La división de nuestra red en subredes o VLANs que agrupen cada uno de estos tipos de tráfico permitirá la aplicación de políticas de seguridad particulares para cada uno de ellos. Además, para mejor la administración de nuestra red, se ha decidido dividir el tráfico de los usuarios cableados con una VLAN por planta, de esta forma mejoraremos el control y administración de la red al tratarse de un volumen de tráfico elevado y disgregado.

Según todos estos criterios, definimos las VLANs y los tipos de tráfico que se muestran en la Tabla 2, teniendo en cuenta que para la definición del identificativo de cada VLAN se ha utilizado una numeración de forma arbitraria.

Id. VLAN	Descripción	Tipo de tráfico
VLAN 10	Red de usuarios cableados planta 0	Tráfico generado por todos los usuarios conectados por cable a los equipos de red de la planta 0
VLAN 11	Red de usuarios cableados planta 1	Tráfico generado por todos los usuarios conectados por cable a los equipos de red de la planta 1
VLAN 12	Red de usuarios cableados planta 2	Tráfico generado por todos los usuarios conectados por cable a los equipos de red de la planta 2

VLAN 13	Red de usuarios cableados planta 3	Tráfico generado por todos los usuarios conectados por cable a los equipos de red de la planta 3
VLAN 14	Red de usuarios cableados planta 4	Tráfico generado por todos los usuarios conectados por cable a los equipos de red de la planta 4
VLAN 20	Red de dispositivos WiFi	Tráfico que generan los dispositivos de la red inalámbrica (WiFi) (puntos de acceso y controladores).
VLAN 21	Red de usuarios WiFi	Tráfico que generan los usuarios que se conectan a la red inalámbrica.
VLAN 22	Red de invitados WiFi	Tráfico que generan los invitados que se conectan a la red inalámbrica.
VLAN 30	Red de gestión	Tráfico de gestión de todos los dispositivos de nuestra red que sean gestionables
VLAN 40	Red de tránsito internet	Tráfico que tiene como destino internet
VLAN 50	Red de videoconferencia	Tráfico que generan los equipos de videoconferencia de nuestra red.
VLAN 60	Red de equipos multifunción	Tráfico que generan los equipos multifunción (impresora, fax y escáner) de nuestra red.

Tabla 2. Definición de VLANs

Este listado de VLANs se completará más adelante en el apartado de *Ampliación de detalles de diseño*, una vez que se haya definido completamente la solución técnica propuesta.

4.2 Red cableada

Para el diseño de la red cableada vamos a considerar una arquitectura de red basada en capas. Este tipo de arquitectura consiste en dividir la red en capas independientes cada una de las cuales tiene unas funciones específicas, la separación de las diferentes funciones específicas permite que el diseño de la red sea modular facilitando la escalabilidad de la solución.

La arquitectura basada en capas más habitual consiste en las siguientes tres capas:

- **Capa de acceso**, proporciona la conectividad a la red de los terminales de usuario.
- **Capa de distribución**, agrega el tráfico recibido de la capa de acceso y controla el tráfico que circula por la red mediante la aplicación de mecanismos de filtrado.
- **Capa de core**, agrega el tráfico que proviene de la capa de distribución y proporciona conectividad a Internet.

En redes pequeñas, es habitual implementar esta arquitectura con la capa de distribución y la capa de core combinadas en una sola capa de distribución/core.

Para nuestra red cableada definimos una arquitectura basada en capas con una capa de acceso y una capa de distribución/core:

- La **capa de acceso** contiene los equipos denominados de acceso con conectividad directa con los dispositivos de usuario. En nuestro caso serán switches de nivel 2 a los cuales se conectarán los terminales de usuarios de cada planta, los dispositivos de videoconferencia y los equipos multifunción (impresora, fax y escáner).
- La **capa de distribución/core** se encuentra encima de la capa de acceso y contiene los equipos de nivel 3 encargados del enrutamiento entre las distintas subredes, los firewalls encargados de la aplicación de políticas de seguridad y el router que proporciona salida a Internet.

La *Figura 6*, muestra de forma gráfica la arquitectura de red empleada para nuestra red cableada:

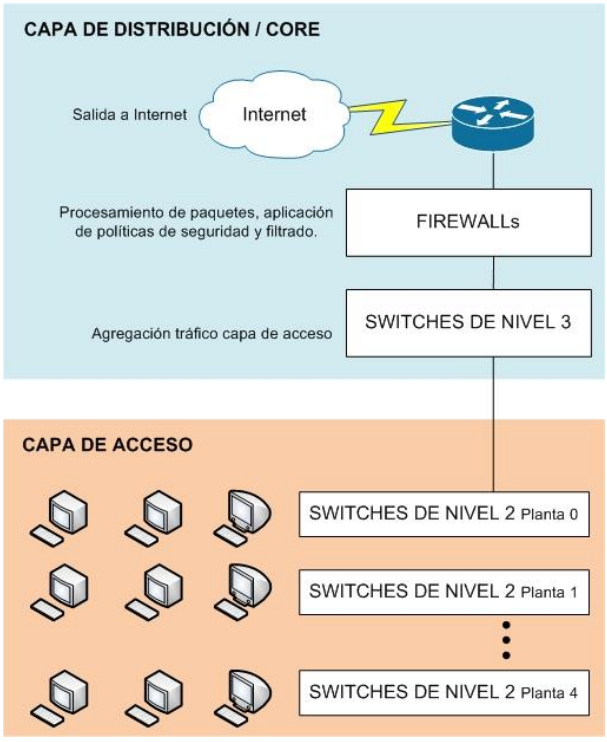


Figura 6. Red Cableada: Arquitectura basada en Capas

A continuación se detallan las particularidades de diseño y el dimensionamiento del equipamiento necesario para cada una de las capas que forman nuestra arquitectura de red.

4.2.1 Capa de acceso

La capa de acceso, está compuesta por switches de acceso de nivel 2 a los cuales se conectarán físicamente los terminales de usuario.

- ***Equipos de acceso: switches de nivel 2***

Para determinar el tipo y número de switches de acceso que necesitamos y la capacidad de los mismos, debemos fijarnos en primer lugar en los datos de volumen de puestos de trabajo por planta definidos en el apartado de caso de estudio.

El número de switches de acceso por planta viene determinado por el total de puestos de trabajo estimados por planta, según se indica en la ecuación (1)

$$(1)\quad \begin{matrix} Nº\ Total \\ Puestos\ Trabajo \\ Estimados\ por\ Planta \end{matrix} = Entero\ Superior\left[\left(\begin{matrix} Nº\ Total \\ Puestos\ Trabajo \\ por\ Planta \end{matrix}\right) + \begin{matrix} \%\ Crecimiento\ Estimado \\ Nº\ de\ Puestos \\ Trabajo\ por\ Planta \end{matrix}\ x\left(\begin{matrix} Nº\ Total \\ Puestos\ Trabajo \\ por\ Planta \end{matrix}\right)\right]$$

Además del número total de puestos de trabajo estimados por planta, los switches de acceso deberán tener capacidad suficiente para la conectividad de los puntos de acceso WiFi necesarios para el despliegue de la red inalámbrica. El diseño de la red inalámbrica se abordará en detalle en el apartado siguiente, por el momento tendremos en cuenta la aproximación que muestra la ecuación (2)

$$(2)\quad \begin{matrix} Aproximación\ nº\ puntos \\ de\ acceso\ por\ planta \end{matrix} = 6$$

Los equipos multifunción (impresora, fax y escáner) son terminales de usuario por lo que también estarán conectados directamente a los switches de acceso, es por ello que debemos considerar los puertos necesarios para la conexión de estos equipos teniendo en cuenta que necesitamos ubicar un equipo multifunción por planta, tal cual se indica en la ecuación (3)

$$(3)\quad \begin{matrix} Nº\ Equipos \\ Multifunción\ por\ planta \end{matrix} = 1$$

Según las ecuaciones (1), (2) y (3) podemos calcular el número total de puertos de switch de acceso por planta, tal cual refleja la ecuación (4)

$$(4)\quad \begin{matrix} Nº\ Total\ Puertos \\ Switch\ Acceso\ por\ Planta \end{matrix} = \begin{matrix} Nº\ Total \\ Puestos\ Trabajo \\ Estimados\ por\ Planta \end{matrix} + 6 + 1$$

En función del número total de puertos por planta, el número de switches de acceso por planta se obtiene según las ecuación (5)

$$(5)\quad \frac{Nº\ Total\ de\ Switches}{de\ Acceso\ por\ Planta} = Entero\ Superior\left[\frac{\frac{Nº\ Total\ Puertos}{Switch\ Acceso\ por\ Planta}}{Nº\ de\ Puertos\ de\ Acceso\ por\ Switch}\right]$$

Por último, debemos tener en cuenta una previsión de puertos para la conectividad de los dos equipos de videoconferencia ubicados en las plantas 0 y 1, para ello consideramos la ecuación (6)

$$(6)\quad \frac{Nº\ Total\ Puertos}{Switch\ Acceso\ Plantas\ 0\ y\ 1} = \frac{Nº\ Total\ Puertos}{Switch\ Acceso\ por\ Planta} + 1$$

Existen diferentes modelos de switches en el mercado con diferentes cantidades de puertos de acceso (8, 12, 24, 48...), para nuestro caso consideraremos switches de 48 puertos.

Aplicando las fórmulas (1), (2), (3), (4), (5) y (6) obtenemos el número total de puestos de trabajo estimados por planta y el número total de switches de acceso por planta tal cual se muestra en la siguiente tabla:

Plantas	Nº puestos de trabajo	% Crecimiento estimado nº de puestos de trabajo	Nº puestos de trabajo estimados	Nº total puertos	Nº puertos acceso por switch	Nº total switches acceso
Planta 0	154	2 %	158	158+6+1+1	48	4
Planta 1	169	1 %	171	171+6+1+1	48	4
Planta 2	186	0 %	187	187+6+1	48	5
Planta 3	186	0 %	187	187+6+1	48	5
Planta 4	118	3 %	122	122+6+1	48	3
TOTALES	**813**	-	**825**	**862**	**-**	**21**

Tabla 3. Switches de acceso por Planta

Para cada planta se instalará un stack o pila de switches apilables entre sí por el total de switches por planta que indica la tabla. De esta forma dispondremos de un stack de 4 switches en las planta 0 y 1, un stack de 5 switches en las planta 2 y 3, y un stack de 3 switches en la planta 4. A nivel de configuración, cada stack de switches será considerado como un único switch con una única dirección IP para su gestión.

La velocidad de los puertos de los switches de acceso o la cantidad de tráfico que deben de ser capaces de procesar viene determinada por la cantidad de tráfico que será generada por los usuarios de la red. Al tratarse de una red con un tráfico heterogéneo y con el objetivo de cubrir las expectativas más altas se han considerado switches con puertos con velocidad de 1 Gigabit por segundo.

Además de los puertos de acceso, la gran mayoría de switches disponibles en el mercado cuentan con mínimo dos puertos dedicados a la conectividad con la capa superior. La velocidad o capacidad de estos puertos deberá ser superior a la capacidad de los puertos de acceso ya que tienen que ser capaces de procesar todo el tráfico que se dirige de una capa a otra. En nuestro caso se han considerado switches de acceso con dos puertos de fibra óptica multi-modo de 10 Gigabits por segundo para la conectividad con la capa de distribución/core.

En cuanto a la funcionalidad de los switches de acceso, únicamente es necesario que direccionen a nivel de enlace el tráfico generado por los usuarios hacia la capa superior, por lo tanto los switches utilizados serán de nivel 2 o nivel de enlace.

- ***Servicio de videoconferencia***

Para ofrecer el servicio de videoconferencia que se detalla en los requisitos del capítulo 3, se dispondrá de dos sistemas de videoconferencia compactos formados por una pantalla de 55 pulgadas, códec y MCU integrada, cámara con zoom 4x y micrófonos de mesa, que serán ubicados en las plantas 0 y 1.

Cada sistema de videoconferencia se conectará físicamente a uno de los switches del stack de switches de la planta 0 y 1 mediante un enlace de cobre a 1Gbps.

- ***Servicio de multifunción (impresora, fax y escáner)***

Para ofrecer el servicio de multifunción que se detalla en los requisitos del capítulo 3, se dispondrá de un equipo multifunción con capacidad de impresora, fax y escáner en cada planta del centro.

Cada equipo multifunción se conectará físicamente a uno de los switches del stack de switches de nivel 2 de su planta mediante un enlace de cobre a 1Gbps.

4.2.2 Capa de distribución/core

La capa de distribución/core se encarga de agregar el tráfico que proviene de la capa de acceso, llevar a cabo el enrutamiento entre las diferentes subredes que forman nuestra red, procesar los paquetes aplicando mecanismos de control y filtrado, y proporcionar salida a Internet.

La Tabla 4 resume el equipamiento que se empleará para cumplir cada una de las funciones de esta capa, el cual será desarrollado a lo largo de este apartado junto con la arquitectura definida para cada equipamiento.

Funciones capa de distribución/core	Tipo de equipamiento con el que se realizará esta función
Agregación del tráfico de la capa de acceso	Switches
Enrutamiento del tráfico entre las diferentes subredes	Firewalls
Procesamiento de paquetes con mecanismos de control y filtrado	
Salida a internet	Routers

Tabla 4. Capa de distribución/core: funciones y tipo de equipamiento

- ***Agregación del tráfico de la capa de acceso: switches de nivel 3***

Para agregar el tráfico que proviene de la capa de acceso utilizaremos **dos switches** en arquitectura de **alta disponibilidad** en modo **activo-activo**, que estarán conectados de forma idéntica a cada stack o pila de switches de la capa de acceso mejorando el rendimiento y la disponibilidad del servicio.

Estos switches tendrán **funcionalidad de nivel 3**, lo cual se justificará más adelante una vez que se haya definido de forma completa la arquitectura de toda la capa de distribución/core; inicialmente consideramos que los switches de la capa de distribución/core únicamente realizarán la agregación del tráfico de los switches de la capa acceso.

Además de los switches de la capa de acceso, a los switches de la capa de distribución/core se conectarán el resto de dispositivos que forman nuestra red y que se irán definiendo en los siguientes apartados. Para determinar el número de puertos de los switches de la capa de distribución/core debemos tener en cuenta las siguientes consideraciones que se irán definiendo en detalle a lo largo del desarrollo de la solución:

- La conectividad de los switches de la capa de distribución/core con los switches de la capa de acceso, se realiza mediante un enlace de fibra óptica multi-modo de 10Gbps desde cada switch de la capa de distribución/core hacia cada stack de switches de acceso.
- Para proporcionar salida a internet, se dispondrá de dos routers, conectados a los switches de la capa de distribución/core mediante enlaces de cobre a 1Gbps.

- Para el enrutamiento entre subredes y la aplicación de políticas de seguridad y filtrado, se dispondrá de dos firewalls conectados a los switches de distribución/core mediante tres enlaces de cobre a 1Gbps por cada Firewall.
- En relación a la red inalámbrica que se desarrollará en apartados posteriores, se dispondrá de dos controladores encargados de la gestión de los puntos de acceso de la red inalámbrica, conectados a la capa de distribución/core mediante dos enlaces de cobre a 1Gbps por cada controlador.

Teniendo en cuenta estas consideraciones podemos determinar el número de puertos necesarios aplicando las ecuaciones (7), (8), (9), (10) y (11):

(7) $$Nº\ Puertos\ Distribución/Core\ para\ conectividad\ con\ capa\ de\ Acceso = Nº\ Stack\ de\ switches\ de\ Acceso\ x\ 2$$

(8) $$Nº\ Puertos\ Distribución\ para\ conectividad\ con\ Routers = Nº\ Routers\ = 2$$

(9) $$Nº\ Puertos\ Distribución\ para\ conectividad\ con\ Firewalls = Nº\ Firewalls\ x\ 3 = 2\ x\ 3 = 6$$

(10) $$Nº\ Puertos\ Distribución\ para\ conectividad\ con\ Controladores\ Wireless = Nº\ Controladores\ Wireless\ = 2\ x\ 2 = 4$$

(11) $$Nº\ Total\ Puertos\ para\ capa\ de\ Distribución = (7) + (8) + (9) + (10)$$

Como resultado de aplicar estas ecuaciones, se obtiene el resumen del tipo y número de puertos necesarios para los switches de la capa de distribución/core que muestra la Tabla 5.

Nº Puertos Fibra Óptica MM 10Gbps para conectividad con capa acceso	Nº Puertos Cobre 1Gbps para conectividad con Routers	Nº Puertos Cobre 1Gbps para conectividad con firewalls	Nº Puertos Cobre 1Gbps para conectividad con Controladoras Inalámbrica
10 (5 x 2)	2	6 (3 x 2)	4
TOTAL puertos Fibra Óptica MM 10Gbps		10	
TOTAL puertos Cobre 1Gbps		12	

Tabla 5. Puertos Switches Distribución/core

Como puede apreciarse en la Tabla 5, necesitamos un total de 22 puertos, 10 de ellos estarán dedicados a enlaces de fibra óptica multi-modo de 10Gbps y los 12 restantes, a enlaces de cobre a 1Gbps. El número total de puertos que se ha obtenido, se repartirá entre los dos switches de distribución/core.

Según estos resultados, con dos switches de 12 puertos cada uno, tendríamos una capacidad total de 24 puertos, la cual sería suficiente para la necesidad de puertos que se ha obtenido. Sin embargo, se ha decidido utilizar dos switches de 24 puertos, lo cual nos proporciona un total de 48 puertos, mejorando así la escalabilidad de nuestra solución en caso de un crecimiento futuro.

El modelo de switch empleado necesitará adaptadores de puerto de un tipo determinado en función del tipo de enlace para el que esté destinado cada puerto. De esta forma, según la previsión de puertos que se ha definido, necesitaremos 10 adaptadores para fibra óptica multi-modo a 10Gbps y 12 de cobre a 1Gbps.

- ***Enrutamiento y procesamiento de paquetes: firewalls***

Según se especificó en el capítulo 3, la red a diseñar debe disponer de mecanismos de seguridad que controlen el tráfico que circule por la red. Para cumplir con este requisito utilizaremos firewalls dentro de la capa de distribución/core que se encarguen del enrutamiento entre las diferentes subredes y además realicen el procesamiento de los paquetes que los atraviesan aplicando mecanismos de control y filtrado.

En concreto emplearemos una arquitectura de **alta disponibilidad** con un cluster de dos firewalls en modo **activo-pasivo.** Mediante esta arquitectura uno de los firewall actuará como principal mientras que el otro se mantendrá inactivo y sólo pasará a estado activo en caso de caída o fallo del firewall principal, mejorando así la disponibilidad y continuidad del servicio. El cluster de firewalls estará conectado a los switches de la capa de distribución/core.

Uno de los aspectos más importantes a la hora de determinar el modelo de firewall idóneo para nuestra red, es la tasa de tráfico que es capaz de procesar. Para determinar la tasa de tráfico que necesitamos que soporte nuestro firewall debemos conocer en primer lugar una aproximación del volumen de tráfico que se generará en nuestra red, en nuestro caso disponemos de una red de aproximadamente 800 usuarios para la que se ha estimado un consumo medio de 1Mbit/s por usuario, por lo que se considera apropiado un firewall con capacidad de procesamiento de 1GBit/s.

En cuanto al número de interfaces físicas del firewall, existen diferentes modelos en el mercado que ofrecen una gran variedad de cantidad de interfaces disponibles. Para determinar el número de interfaces de nuestros firewalls que más se ajusta a nuestras necesidades, debemos considerar el número de subredes o VLANs que van a ser configuradas en los firewalls y decidir la distribución de cada subred o VLAN por cada interfaz del firewall en función de la cantidad de tráfico esperada para cada una de ellas y teniendo en cuenta que es posible configurar una misma interfaz para más de una VLAN dividiendo la interfaz en varias subinterfaces.

El detalle del número de VLANs configuradas por cada interfaz o subinterfaz del firewall y por lo tanto del número de interfaces de cada firewall, se incluirá más adelante dentro del apartado de Ampliación de detalles de diseño, una vez que se haya definido completamente la solución técnica propuesta.

Por último, es importante definir las funcionalidades de nuestro firewall. Por lo general, todos los modelos de firewalls tienen diferentes paquetes de software que se habilitan a través de la adquisición de una licencia y que determinan las funcionalidades o capacidades del mismo. Es importante adquirir sólo aquellas funcionalidades que realmente necesitemos para no sobrecargar al Firewall de procesamiento innecesario que le limite en su rendimiento. En nuestro caso, necesitamos un dispositivo de Firewall que cuente con las siguientes funcionalidades:

- Funcionalidad de firewall o funcionalidad básica: permite la aplicación de reglas de acceso y el mecanismo NAT (Network Address Translation)
- Funcionalidad IPS: Inspecciona patrones de tráfico para detectar posibles ataques.
- Funcionalidad de control de aplicación: Permite la aplicación de restricciones por aplicación
- Funcionalidad de filtrado por URL: Permite disponer de una base de datos con las URLs más comunes, pudiendo así aplicar restricciones por categorías de URLs

- ***Salida a Internet: routers***

Por último, la capa de distribución/core se encarga de proporcionar la salida a internet. Para ello se dispondrá de dos routers conectados uno a cada uno de los switches de nivel 3, con el fin de garantizar que la salida a internet esté disponible incluso si se produce una caída o fallo en uno de los switches.

Para el desarrollo del presente proyecto se considera que los routers para proporcionar la salida a internet serán proporcionados por el proveedor de Internet, por lo que no es

necesaria ninguna previsión de equipamiento o definición de arquitectura dentro de este apartado.

4.3 Red inalámbrica

La red inalámbrica que pretendemos diseñar estará formada por una sería de dispositivos de acceso al medio inalámbrico o **puntos de acceso**.

Además, para el diseño de nuestra red inalámbrica vamos a considerar una **arquitectura de red inalámbrica centralizada**. Esta arquitectura se basa en centralizar la gestión de todos los puntos de acceso que forman nuestra red inalámbrica en un dispositivo denominado controlador. En nuestro caso, utilizaremos una configuración de **alta disponibilidad** con **dos controladores** en **modo activo-pasivo**.

De esta forma, se dispondrá de una serie de puntos de acceso distribuidos por cada planta conectados físicamente a los switches de acceso, y dos controladores en alta disponibilidad y modo activo-pasivo encargados de la gestión de los puntos de acceso que estarán conectados a los switches de la capa de distribución/core, como muestra la figura 7.

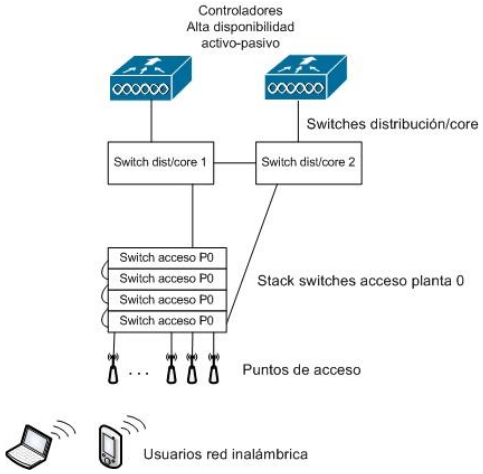


Figura 7. Red Inalámbrica: Arquitectura Centralizada

La principal ventaja de utilizar una arquitectura de red centralizada es la facilidad en la administración de la red. En el caso de una arquitectura de red inalámbrica no centralizada, cada punto de acceso tiene que ser gestionado de forma individual, lo cual supone un mayor consumo de tiempo.

Para realizar el diseño de nuestra red inalámbrica, en primer lugar debemos determinar el número de puntos de acceso necesarios por cada planta para garantizar la cobertura en toda

la superficie de nuestro centro. Para ello se ha realizado la simulación de un estudio de cobertura inalámbrica, tal cual se describe en el siguiente apartado.

4.3.1 Simulación estudio de cobertura

Para la realización de la simulación del estudio de cobertura inalámbrica se ha utilizado el software *Ekahau site survey 6.0.*

Figura 8. Ekahau site survey 6.0

A continuación se detallan los pasos seguidos en la realización del estudio.

1. Añadir planos

El primer paso una vez iniciado el programa *Ekahau site survey 6.0,* es cargar en el mismo todos los planos de planta sobre los que vamos a realizar el estudio.

Si observamos los planos de planta incluidos en la definición de nuestro caso de estudio, vemos que todas las plantas tienen la misma superficie; además, las plantas 0 y 1 son idénticas entre sí, al igual que ocurre con las plantas 2 y 3. Esto nos permite poder realizar el estudio únicamente en las plantas 0, 2 y 4, y extrapolar los resultados obtenidos al resto de plantas.

Alcance estudio de cobertura	Comentarios
Planta 0	Extrapolación de resultados a Planta 1
Planta 2	Extrapolación de resultados a Planta 3
Planta 4	-

Tabla 6. Alcance estudio de cobertura

2. Definir escala

Una vez que hemos añadido los planos de las plantas 0, 2 y 4, el siguiente paso es definir la escala de nuestros planos. Para ello, vamos a tomar una medida conocida como es el ancho del marco de una puerta cuyas dimensiones suelen ser de 90cm. Con la función "*ruler*" trazamos una línea sobre el ancho de una puerta de nuestro plano y fijamos la dimensión a

90cm como muestra la figura 9, de esta forma ya queda definida la escala de nuestro plano. Repetimos esta misma acción con todos los planos de planta.

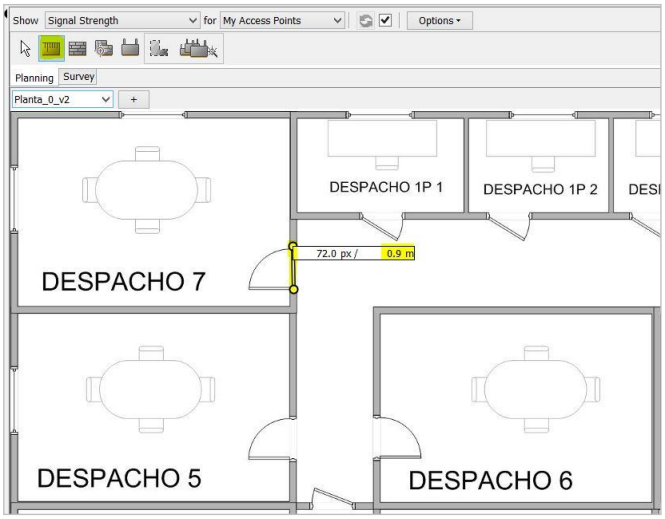


Figura 9. Definición de la escala de los planos

3. Indicar materiales

El siguiente paso consiste en indicar los materiales de todas las superficies que dividen los espacios de cada planta (paredes, puertas, ventanas, etc.), no será necesario reflejar los materiales de las superficies de poca altura, como mesas, sillas, sofás, macetas, etc, ya que los puntos de acceso serán ubicados en el techo y por lo tanto los objetos de poca altura no afectarán a la propagación de la señal.

El software *Ekahau site survey* permite la selección de varios tipos de materiales como ladrillo, diferentes tipos de madera, hormigón, mármol, cristal fino y grueso etc. Cada uno de estos materiales por sus componentes y propiedades que los definen, tienen un nivel de absorción de las ondas electromagnéticas determinado, de tal forma que la propagación de la señal se ve afectada por el tipo de materiales que se encuentra a su paso.

Para la simulación de nuestro estudio, debemos intentar reflejar de la manera más real posible todos los materiales de las superficies de nuestras plantas. La figura 10 muestra la función a seleccionar y el resultado del plano una vez que se han indicado sobre el mismo todos los materiales.

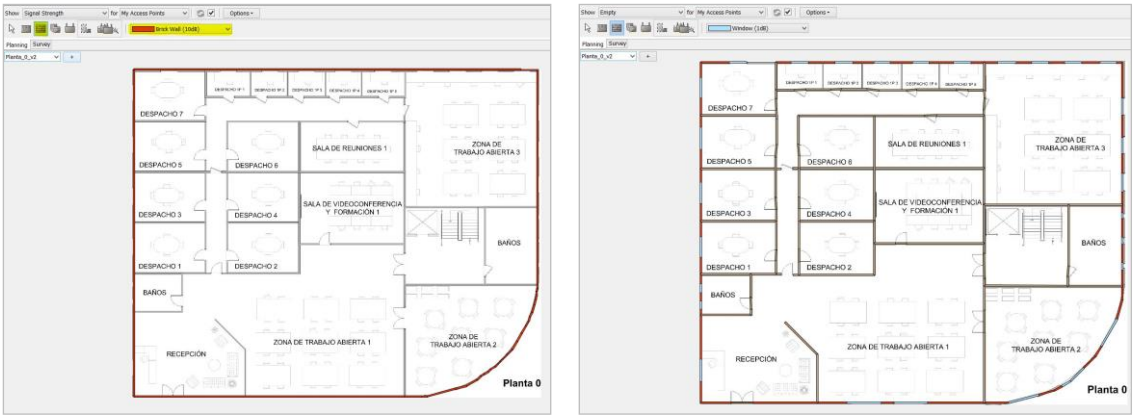


Figura 10. Definición de materiales

4. Área de cobertura

Después de establecer todos los materiales de todas las superficies de los planos, el siguiente paso consiste en determinar el área sobre la que queremos tener cobertura Wi-Fi y por lo tanto queremos realizar el estudio. En nuestro caso, vamos a considerar como área de cobertura, toda la superficie de planta a excepción de los baños y la cocina ubicada en la planta cuarta. La figura 11 muestra el resultado de marcar todo el área de aplicación del estudio en la planta 0.

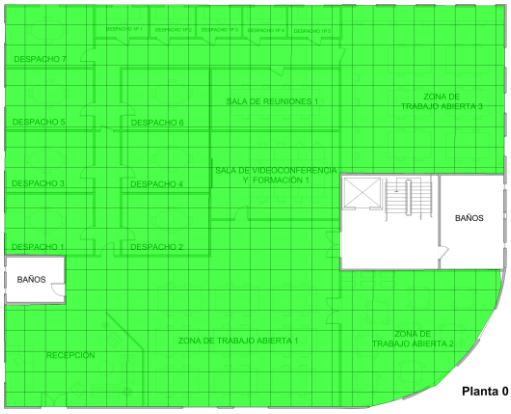


Figura 11. Definir área de cobertura

5. Auto-Planner: definición de requisitos y tipo de puntos de acceso.

Una vez que tenemos definida la escala de los planos, los materiales de las superficies y el área de cobertura, debemos definir nuestros requerimientos de cobertura y capacidad, así como el tipo de puntos de acceso, estándar Wi-Fi y frecuencia sobre la que vamos a trabajar. Todos estos parámetros se definen mediante la función Auto-Planner, y es el paso final previo a obtener nuestro estudio de cobertura simulado mediante software.

La figura 12 muestra el detalle de la función Auto-Planner.

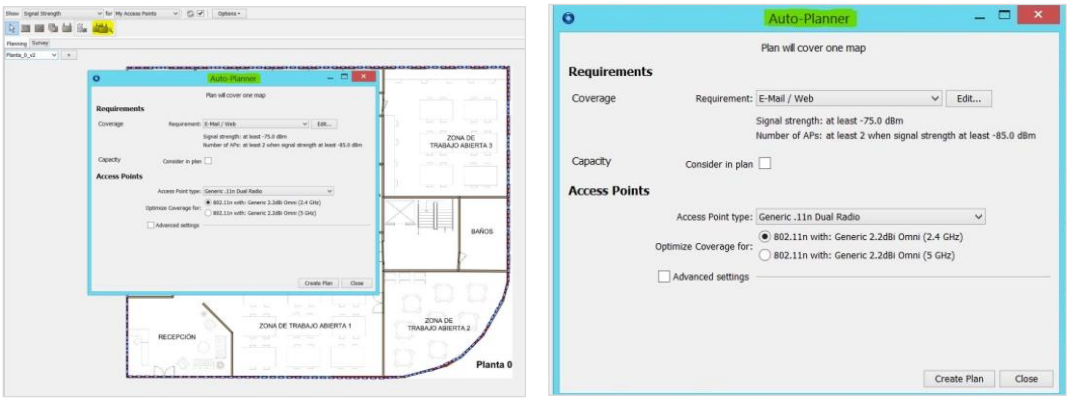


Figura 12. Función Auto-Planner

Para el diseño de nuestra red inalámbrica se tienen en cuenta las siguientes consideraciones que serán configuradas dentro de la función Auto-Planner:

- El tráfico transmitido a través de la red inalámbrica será solo tráfico de datos (E-Mail/Web), no se considera la transmisión de tráfico de voz.
- La infraestructura empleada para el diseño soportará el último estándar IEEE 802.11ac que permite alcanzar tasas de transmisión de hasta 1,3Gbit/s.

El software *Ekahau site survey* tiene preestablecidos una serie de valores ideales para el tipo de tráfico de datos (E-Mail/Web), los cuales se muestran en la figura 13.

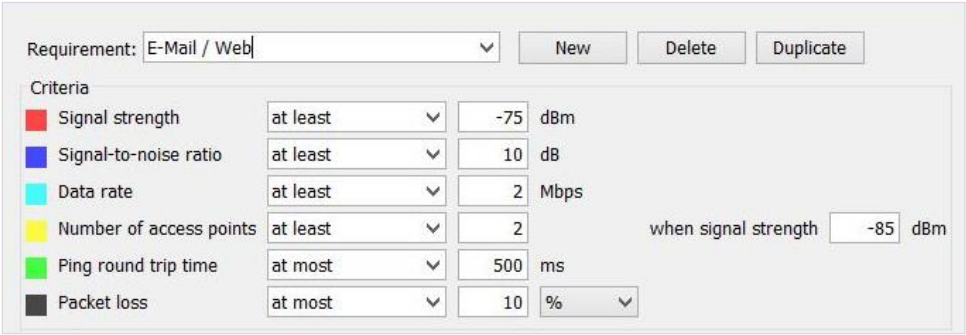


Figura 13. Valores predefinidos tipo de tráfico: E-Mail/Web

Además de los requisitos en cuanto al tipo de tráfico, debemos definir los requisitos en cuanto a la capacidad de nuestra red inalámbrica. Para ello, debemos definir el número de dispositivos o clientes Wi-Fi que se conectarán a nuestra red.

Se ha estimado el siguiente volumen de clientes Wi-Fi en media para todas las plantas:

Tipo de clientes	Nº clientes
PCs Portátiles 802.11ac	165

Disp. smartphones 802.11ac	100
Disp. tablets 802.11ac	25

Tabla 7. Volumen y tipo de clientes red inalámbrica

La figura 14 muestra la definición de los diferentes tipos de clientes que se estiman para nuestra red inalámbrica dentro de la función Auto-Planner.

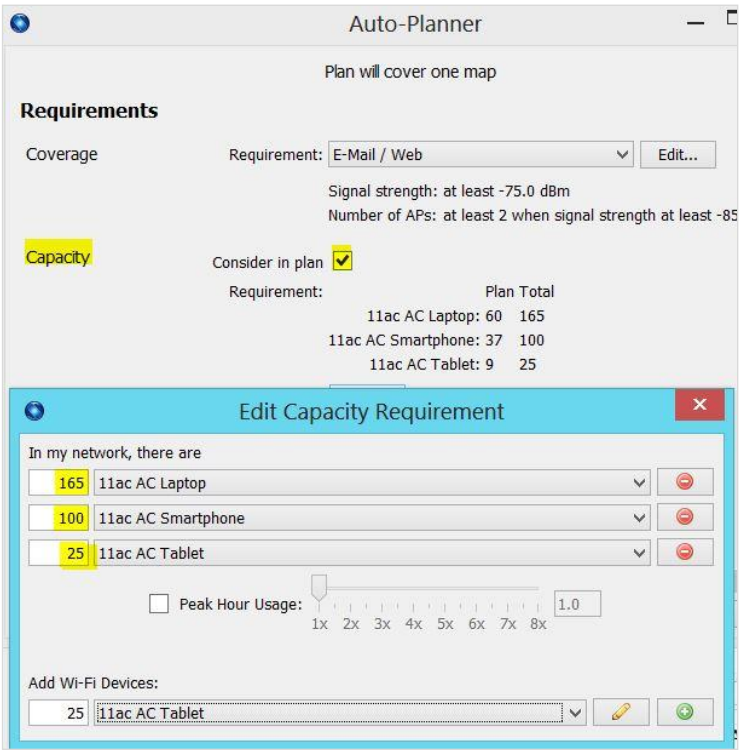


Figura 14. Capacidad (nº/tipo clientes red inalámbrica)

Después de definir los requisitos de cobertura y capacidad, definimos el tipo de puntos de acceso que vamos a emplear para el despliegue de nuestra red inalámbrica. Se van a considerar puntos de acceso de la última tecnología 802.11ac con la cual los puntos de acceso emiten en la banda de los 5GHz y pueden llegar a alcanzar tasas de transmisión de hasta 1,3Gbit/s. La figura 15 muestra la selección del tipo de puntos de acceso que se van a considerar.

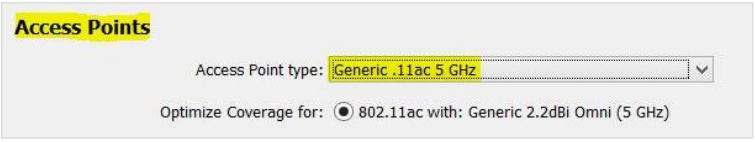


Figura 15. Tipo de puntos de acceso

Además, también podemos definir otras características como son la potencia de transmisión, la altura estimada a la que serán ubicados los puntos de acceso y el ancho de banda en el que operarán. El software *Ekahau site survey* establece los valores por defecto que muestra la figura 16:

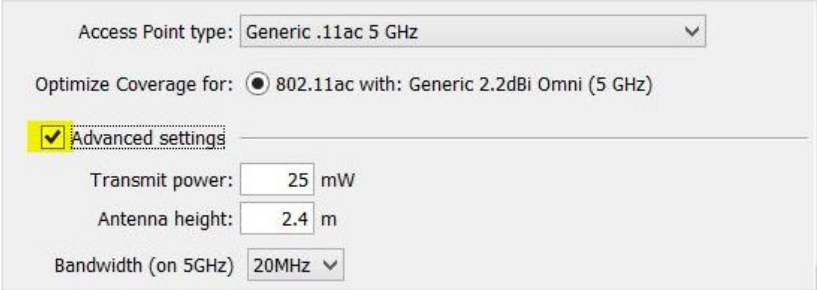


Figura 16. Características puntos de acceso (Auto-Planner)

Para finalizar lanzamos la generación del estudio de cobertura. Mediante esta función, el software *Ekahau site survey* realizará una simulación en base a los planos, materiales de las superficies, área de cobertura, requisitos (cobertura, y capacidad) y tipo de puntos de acceso que se han definido, dando como resultado una simulación completa que incluye como reportes más importantes, los siguientes:

- Ubicación sobre plano de los puntos de acceso.
- Mapa de cobertura o potencia de la señal.
- Mapa de relación señal a ruido.
- Nivel de interferencia.

6. Resultados

A continuación se muestran los resultados del estudio de cobertura realizado en las plantas 0, 2 y 4.

Planta 0

Para la planta 0, se obtienen los resultados que se muestran en las figuras 17, 18, 19 y 20, todos estos resultados son extrapolables a la planta 1 como se justificó al comienzo de este apartado.

- ***Número de puntos de acceso y ubicaciones sobre plano:*** La simulación del estudio de cobertura sobre la planta 0, da como resultado **6 puntos de acceso** distribuidos como muestra la figura 17, con un punto de acceso sobre cada una de las zonas de mayor densidad de puestos de trabajo (zona de trabajo abierta 1, zona de trabajo abierta 2, zona de trabajo abierta 3) con el fin de asegurar un buen nivel de señal en dichas zonas en las que se espera que el volumen de personas trabajando sea mayor que en el resto de zonas de la planta.

Figura 17. Nº puntos de acceso planta 0

- Mapa de cobertura y potencia de la señal: El mapa de cobertura muestra la potencia de la señal recibida a lo largo de toda la superficie. Como puede apreciarse en la figura 18, en las zonas donde se ha estimado la ubicación de los puntos de acceso, la potencia de la señal recibida es mayor, estando cerca de los -20dBm, a media que nos alejamos de los puntos de acceso, la potencia de la señal disminuye. El mapa de cobertura resultante presenta niveles muy buenos en toda la superficie.

Figura 18. Mapa de cobertura planta 0

- Mapa de relación señal a ruido: El mapa de relación señal a ruido muestra la relación entre la potencia de la señal y el ruido generado por las interferencias entre canales. Para evitar la pérdida de paquetes o datos transmitidos, la potencia de la señal recibida siempre debe ser mayor al ruido, es decir, la relación señal a ruido debe ser mayor a cero. Como se aprecia en la figura 19, la relación señal a ruido obtenida es muy buena en toda la superficie de la planta, estando cerca de los 50dB en prácticamente toda la superficie.

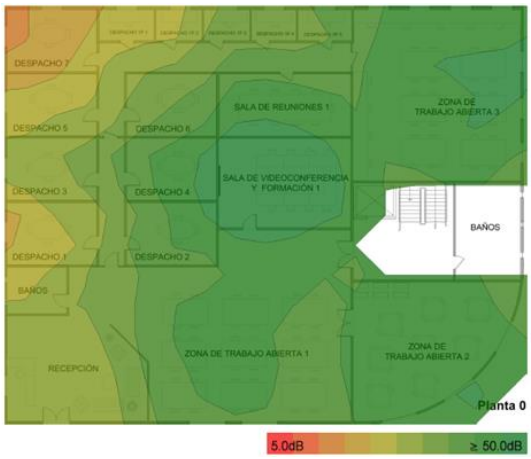


Figura 19. Mapa de relación señal a ruido

- Nivel de interferencia: El gráfico de interferencia, muestra el nivel de interferencia producido por los propios puntos de acceso entre sí al compartir el medio y emitir todos en la misma frecuencia (5GHz) y mismo canal o canales adyacentes. Como se puede apreciar en la figura 20, el nivel de interferencia obtenido es muy bajo, resultando casi despreciable. Podemos apreciar como aquellas zonas donde el nivel de interferencia es ligeramente peor son zonas más diáfanas, de manera que es más probable que las señales emitidas por los puntos de acceso interfieran entre sí.

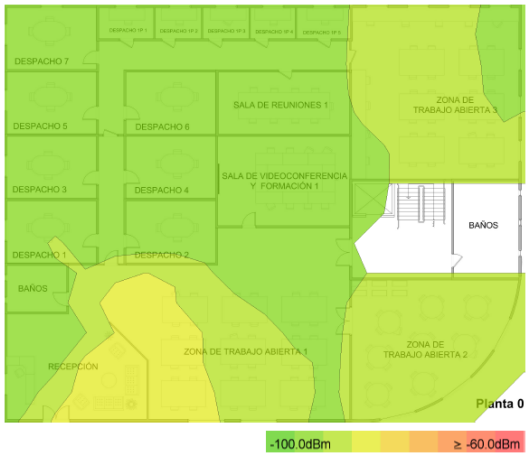


Figura 20. Nivel de interferencia planta 0

Planta 2

Para la planta 2, se obtienen los resultados que se muestran en las figuras 21, 22, 23 y 24, todos estos resultados son extrapolables a la planta 3, como se justificó al comienzo de este apartado.

- Número de puntos de acceso y ubicaciones sobre plano: La simulación del estudio de cobertura sobre la planta 2, da como resultado **5 puntos de acceso** distribuidos según muestra la figura 21. Si comparamos estos resultados con los obtenidos para la planta 0,

vemos que teniendo ambas plantas la misma superficie, debido a que la planta 2 es más diáfana, nos es posible cubrir toda la superficie utilizando un punto de acceso menos que en la planta 0.

Figura 21. Nº puntos de acceso planta 1

- Mapa de cobertura y potencia de la señal: En el mapa de cobertura obtenido para la planta 2 y que se muestra en la figura 22, podemos apreciar como sobre las zonas en las que se han ubicado los puntos de acceso el nivel de señal recibida es mayor. Al igual que en la planta 0 se ha intentado ubicar un punto de acceso para cada una de las zonas de mayor densidad de usuarios para asegurar así la calidad y disponibilidad del servicio en las zonas más críticas.

Figura 22. Mapa de relación señal a ruido

- Mapa de relación señal a ruido: El mapa de relación señal a ruido que se obtiene para la planta 2 y que muestra la figura 23, ofrece valores muy buenos en toda la superficie debido a que la potencia de la señal es muy buena y no existen problemas graves de interferencias entre puntos de acceso.

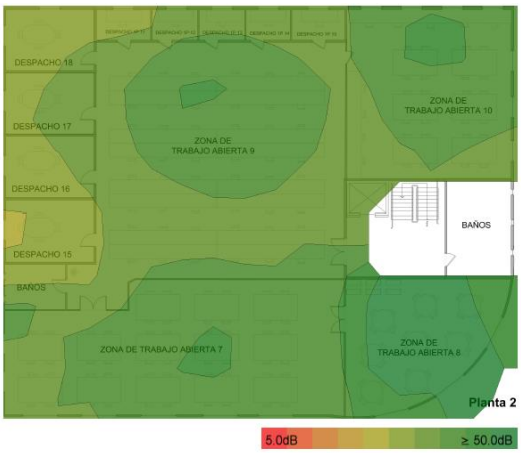


Figura 23. Mapa de relación señal a ruido

- Nivel de interferencia: El gráfico de interferencia que se obtiene para la planta 2 y que muestra la figura 24, refleja como el nivel de interferencia obtenido es muy bajo en toda la superficie del plano, resultando casi despreciable. La parte central del plano muestra valores de interferencia un poco más altos debido a que la superficie en esta zona presenta espacios más diáfanos que facilitan que las ondas emitidas por los puntos de acceso interfieran entre sí.

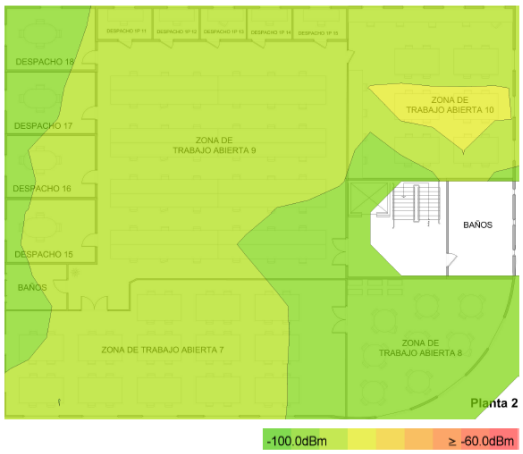


Figura 24. Nivel de interferencia

Planta 4

Para la planta 4, se obtienen los resultados que se muestran en las figuras 25, 26, 27 y 28.

- Número de puntos de acceso y ubicaciones sobre plano: Al igual que en la planta 2, el estudio de cobertura de la planta 4 da como resultado **5 puntos de acceso**. En comparación con las plantas anteriores, la planta 4 es muy similar en cuanto a espacios diáfanos con la planta 2 por lo que los resultados obtenidos serán similares. La figura 26 muestra la ubicación de los puntos de acceso obtenidos para la planta 4.

Figura 25. Nº puntos de acceso planta 4

- Mapa de cobertura y potencia de la señal: El mapa de cobertura obtenido para la planta 4 y que muestra la figura 27 es muy similar a los obtenidos para las plantas anteriores. Los niveles de potencia recibidos son muy buenos en toda la superficie del plano, siendo aún mejores alrededor de las zonas en las que se estima la ubicación de los puntos de acceso.

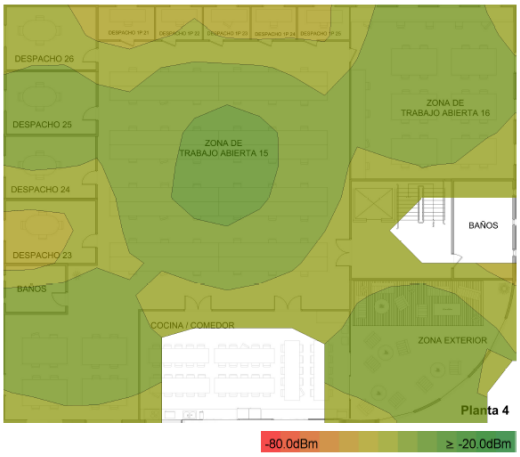


Figura 26. Mapa de cobertura planta 4

- Mapa de relación señal a ruido: El mapa de relación señal a ruido obtenido para la planta 4 y que muestra la figura 28, refleja valores cercanos a los 50dB en prácticamente toda la superficie, dado que los niveles de potencia de la señal recibida son muy altos como pudo verse en el gráfico anterior.

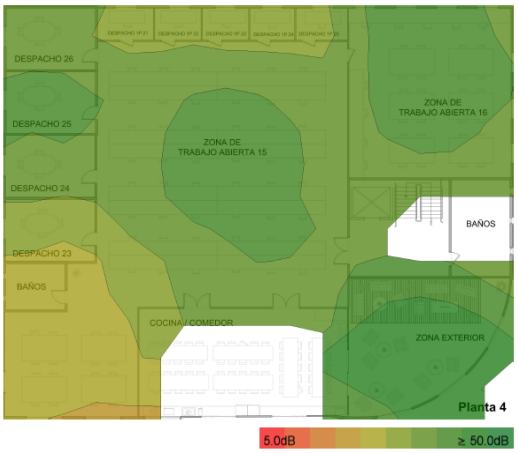


Figura 27. Mapa de relación señal a ruido.

- Nivel de interferencia: El gráfico de interferencia que se obtiene para la planta 4 y que muestra la figura 29, muestra niveles de interferencia muy bajos en toda la superficie del plano. Al igual que en la Planta 2, existen mayores niveles de interferencia en las zonas más diáfanas (zona central del plano), debido a que las ondas emitidas por los puntos de acceso de esa zona interfieren más entre sí.

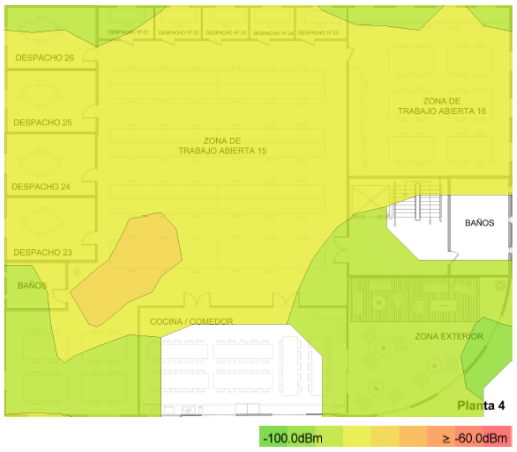


Figura 28. Nivel de interferencia planta

4.3.1.1 Puntos de acceso y controladores

Como resultado de la simulación del estudio de cobertura sobre plano obtenemos la distribución de puntos de acceso necesarios por planta que muestra la Tabla 8.

Planta	Nº puntos de acceso
Planta 0	6
Planta 1	6
Planta 2	5

Planta 3	5
Planta 4	5
TOTAL	**27**

Tabla 8. puntos de acceso por planta

Los puntos de acceso se conectarán físicamente a los switches de la capa de acceso ubicados en cada planta mediante enlaces de cobre a 1Gbps.

Para la gestión centralizada de los 27 puntos de acceso, se utilizará un esquema de **alta disponibilidad** con dos controladores en **modo activo-pasivo**. El número total de puntos de acceso que forman nuestra red inalámbrica, determina la capacidad mínima de los controladores encargados de su gestión, según se indica en la ecuación (12):

$$\text{(12)}\ \frac{Capacidad\ Mínima\ de\ Gestión}{del\ Controlador\ Wireless} = Nº\ Total\ Puntos\ de\ Acceso$$

Para facilitar la escalabilidad de la solución se utilizarán controladores con capacidad de gestión de hasta 50 puntos de acceso de base con posibilidad de ampliar esta capacidad hasta un total de 500 puntos de acceso.

La configuración del esquema de alta disponibilidad de los controladores de puntos de acceso permite que sólo el controlador principal disponga del total de las licencias necesarias, en nuestro caso se ha decidido que sean 50 licencias de base. En caso de caída del controlador principal, el controlador pasivo pasará a adquirir todas las licencias y a establecerse como controlador activo garantizando así la continuidad del servicio.

Los controladores se conectarán físicamente a los switches de la capa de distribución/core mediante enlaces de cobre a 1Gbps por cada controlador.

El resumen de equipamiento Inalámbrica es el siguiente:

Equipamiento Inalámbrica	Cant.
Puntos de acceso	27
Controladores (50 lic Base)	2

Tabla 9. Equipamiento red inalámbrica

4.3.2 Resumen del Equipamiento

La tabla 10 ofrece un resumen de todo el equipamiento descrito en los apartados anteriores y que forma la infraestructura completa de nuestra red.

Equipamiento	Cantidad
Switches capa de acceso (nivel 2)	
Switches nivel 2, 48 puertos, velocidad de puertos 1Gbps. 2 Puertos de 10Gbps con Fibra Óptica MultiModo para conectividad con los switches de nivel 3.	21
Módulos para Fibra Óptica MultiModo a 10Gbps	10
Switches capa distribución/core (nivel 3)	
Switches nivel 3, 24 puertos (adaptador por puerto)	2
Adaptador para Fibra Óptica MultiModo a 10Gbps	10
Adaptador para Cobre a 1Gbps	12
Firewalls	
Firewall	2
Dispositivos red inalámbrica	
Controladores con licencia de base para 50 puntos de acceso (posibilidad de ampliación hasta 500 licencias)	2
Puntos de acceso 802.11 ac. 5 GHz. antenas integradas	27
Equipamiento videoconferencia	
Equipo Videoconferencia con Pantalla de 55”, cámara zoom 4x, micrófonos de mesa y capacidad de videoconferencia múltiple y llamadas externas de hasta tres participantes simultáneamente	2
Equipamiento Multifunción	
Equipo multifunción (impresora, fax y escáner)	5

Tabla 10. Resumen de Equipamiento

4.4 Ampliación de detalles de diseño

El objetivo de este apartado es completar los detalles de diseño de nuestra red que no han sido definidos en los apartados anteriores. Para ello, se desarrollan los siguientes apartados:

- Definición de diseño y diagrama lógico. Se describirá el diseño lógico completo de la red, agrupando y completando los detalles de diseño que se han ido describiendo en cada uno de los apartados anteriores, y representando el resultado del diseño mediante un diagrama o esquema lógico.
- Plan de direccionamiento IP: Se definirá el plan de direccionamiento IP de nuestra red.

4.4.1 Definición de diseño y diagrama lógico

En los apartados anteriores se ha descrito la arquitectura de nuestra **red cableada** como una **arquitectura basada en capas** con una capa de acceso, con un stack o pila de switches por planta para la conectividad de los usuarios cableados, y una capa de distribución/core con dos switches en alta disponibilidad para la agregación del tráfico de los switches de acceso, dos firewalls también en alta disponibilidad para el enrutamiento entre subredes y la aplicación de políticas de seguridad y dos routers para la salida a internet.

Además, sobre esta arquitectura se ha añadido la infraestructura de nuestra **red inalámbrica**, la cual consta de una serie de puntos de acceso por planta conectados a los stack de switches de acceso de cada planta y dos controladores en alta disponibilidad para la **gestión centralizada** de los puntos de acceso, conectados a los switches de distribución/core.

Toda la arquitectura de red descrita hasta el momento se muestra en la figura 29:

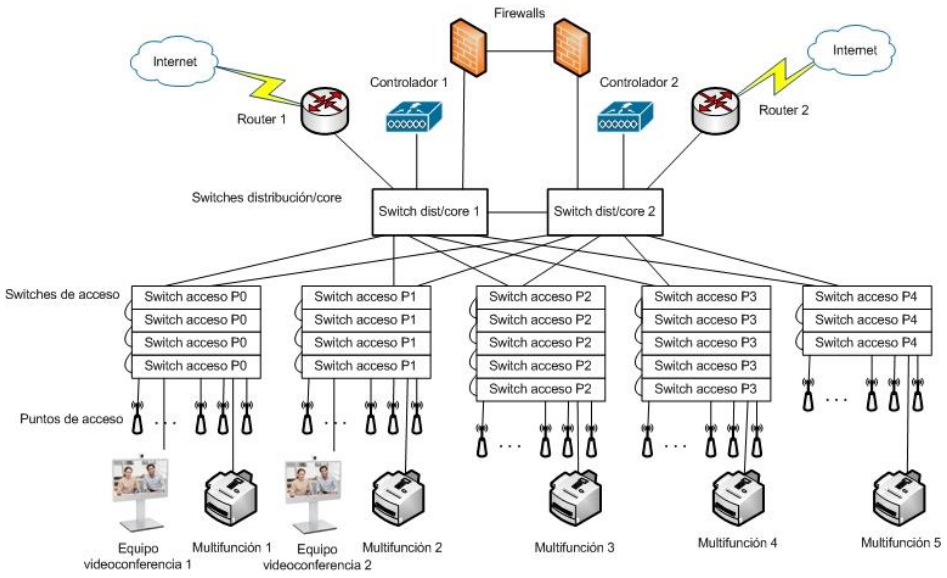


Figura 29. Arquitectura de red

La figura anterior muestra la **arquitectura física** de nuestra red, lo cual nos da información de todos los equipos de red existentes y cómo estos equipos se conectan físicamente entre sí. Para entender cómo se produce el flujo del tráfico dentro de nuestra red, debemos definir la **arquitectura lógica** de la misma. Una manera de definir la arquitectura lógica es elaborando un diagrama o esquema lógico, que consiste en una representación gráfica de la división de nuestra red en subredes lógicas y bloques funcionales que nos ayudan a definir cómo se produce el enrutamiento y flujo del tráfico.

Por lo tanto, el objetivo de la elaboración de un esquema o diagrama lógico es mostrar de una forma gráfica cómo se produce el flujo del tráfico que es enviado desde un punto a otro de la red. Atendiendo a este objetivo, el elemento central de nuestro diagrama lógico debe ser el elemento por el que debe pasar todo el tráfico de la red para poder llegar a su dirección destino, es decir, el elemento que realiza el enrutamiento entre las diferentes subredes que conforman nuestra red. Como se ha definido en los apartados anteriores, este elemento será el **firewall**, que además de realizar el enrutamiento entre subredes, procesará los paquetes aplicando políticas de control y filtrado.

A efectos físicos dispondremos de dos firewalls en configuración de alta disponibilidad activo-pasivo, pero a efectos lógicos nos referiremos al cluster de firewall como un elemento único y lo denotaremos como firewall.

El firewall como elemento central de nuestro diagrama lógico será atravesado por los diferentes tipos de tráfico existentes en nuestra red para así dirigirlos a su destino siempre y cuando cumplan las políticas de seguridad definidas para ellos. Como vimos en el apartado de planteamiento inicial de diseño, se ha decidido dividir nuestra red en las siguientes subredes lógicas o VLANs en función de los diferentes tipos de tráfico que contendrán cada una de ellas:

- VLAN 10: Tráfico de usuarios cableados planta 0
- VLAN 11: Tráfico de usuarios cableados planta 1
- VLAN 12: Tráfico de usuarios cableados planta 2
- VLAN 13: Tráfico de usuarios cableados planta 3
- VLAN 14: Tráfico de usuarios cableados planta 4
- VLAN 20: Tráfico de dispositivos WiFi
- VLAN 21: Tráfico de usuarios WiFi
- VLAN 22: Tráfico de invitados WiFi
- VLAN 30: Tráfico de gestión
- VLAN 40: Tráfico de tránsito a internet
- VLAN 50: Tráfico de videoconferencia
- VLAN 60: Tráfico de equipos multifunción

El firewall centralizará todo el tráfico de las diferentes subredes o VLANs y se encargará del enrutamiento y procesamiento de los paquetes, es por ello que en la elaboración de nuestro diagrama lógico situaremos el firewall en el centro y colgando del mismo representaremos todas las VLANs que se han definido previamente. Para que el esquema resulte más intuitivo, se ha separado la VLAN de tránsito de internet del resto, ubicándola en la parte superior y añadiendo un router y una nube representando la salida a internet. La figura 30 muestra el resultado de esta primera aproximación de diagrama lógico.

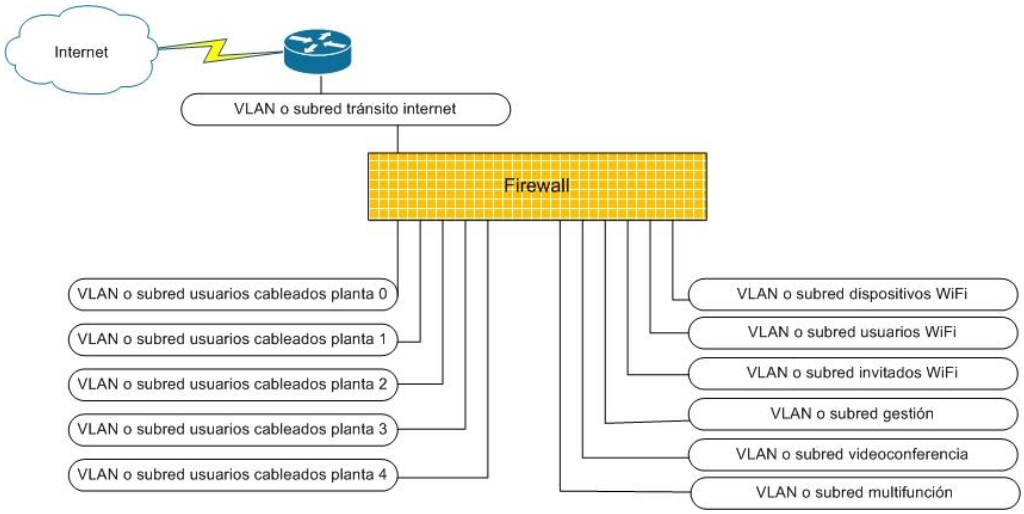


Figura 30. Primera aproximación diagrama lógico

El diagrama que muestra la figura 30 representa como todos los paquetes que provengan de cualquiera de las subredes que cuelgan del firewall deberán atravesar el mismo para poder dirigirse a otra subred. De esta forma, el firewall será el encargado de enrutar los paquetes que vayan de una subred a otra, aplicando las políticas de control y filtrado que se hayan configurado para cada tráfico.

Como ejemplo, si un usuario que pertenezca a la VLAN de invitados WiFi envía tráfico para acceder a un recurso compartido ubicado dentro de la VLAN de usuarios cableados de la planta 3, este tráfico será procesado por el firewall el cual probablemente tenga aplicadas políticas de seguridad y filtrado que limiten el acceso a los recursos de los usuarios corporativos por parte de los usuarios de la VLAN de invitados WiFi. Igualmente, si un usuario que pertenece a la red de usuarios cableada de la planta 4 envía un paquete a un usuario de la red de usuarios cableada de la planta 0, este paquete será procesado y enrutado por el firewall.

Según esta primera aproximación de diagrama lógico, el firewall enrutará y procesará el tráfico de todas las subredes. Si pensamos en las restricciones o políticas de control y filtrado que se aplicarán a cada subred, éstas serán distintas para cada una de las subredes, a excepción de para las subredes de usuarios cableados de cada planta, las cuales tendrán las

mismas políticas configuradas en el firewall. Es decir, **no se establecerá ninguna distinción entre las políticas de seguridad a aplicar para cada una de las subredes de usuarios cableados de cada planta ni tampoco restricciones en cuanto a la comunicación entre estas subredes.**

Esto implica que si hacemos que todas las subredes de usuarios cableados de cada planta cuelguen directamente del firewall, querrá decir que a nivel de configuración en el firewall se deberán de replicar las mismas reglas o políticas de seguridad idénticas para cada una de las subredes cableadas de cada planta. Esto supone sobrecargar al firewall con un procesamiento innecesario, ya que a nivel de reglas y políticas de seguridad, todas las subredes de usuarios de cada planta se podrían tratar como una misma subred.

Para solucionar esta situación y evitar sobrecargar de tareas de procesamiento al firewall, liberaremos al firewall de las tareas de procesamiento y enrutamiento entre las subredes cableadas de planta y asignaremos esta función a los switches de nivel 3 de la capa de distribución/core.

Aplicando esta decisión de diseño, los firewalls se encargarán del enrutamiento entre todas las subredes a excepción únicamente del enrutamiento entre las subredes de usuarios cableados de cada planta, cuyo enrutamiento lo llevarán a cabo los switches de nivel 3 de la capa de distribución/core.

Para identificar de manera lógica todo el tráfico que va desde los switches de nivel 3 de la capa de ditribución/core al firewall definimos una subred lógica o **VLAN de transito dedicada al tráfico de tránsito de usuarios**, a la cual le asignaremos la nomenclatura de **VLAN 70**

A continuación se muestra el diagrama lógico resultante:

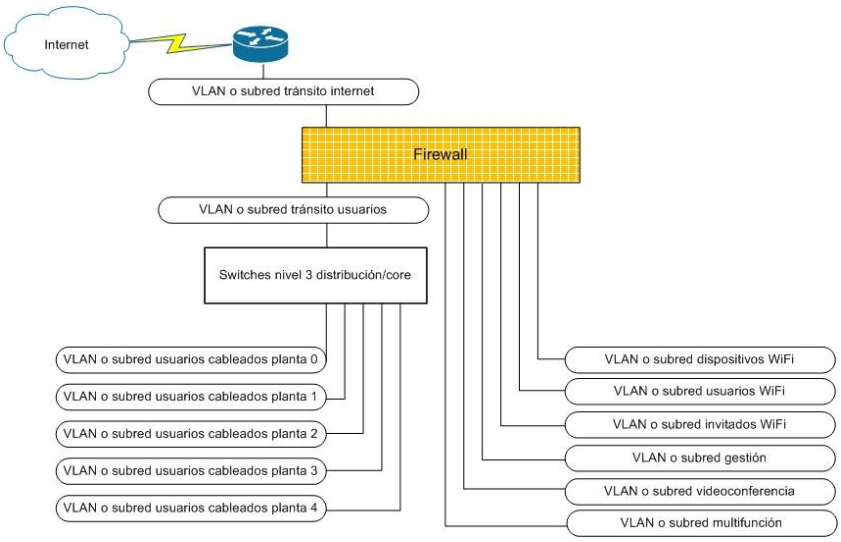


Figura 31. Diagrama Lógico

Como vimos en apartados anteriores, el número de interfaces de firewall necesarias puede calcularse teniendo en cuenta las VLANs que serán configuradas en los firewalls y la distribución de las mismas entre estas interfaces o subinterfaces en función del volumen de tráfico que se estima para cada una de ellas.

El listado definitivo de VLANs que serán configuradas en los firewalls se indican a continuación en la Tabla 11:

VLAN	Descripción	TIPO DE TRÁFICO
VLAN 20	Red Dispositivos WiFi	Tráfico entre puntos de acceso y controladora inalámbrica
VLAN 21	Red usuarios WiFi	Tráfico de usuarios de la red WiFi
VLAN 22	Red invitados WiFi	Tráfico de invitados de la red WiFi
VLAN 30	Red de Gestión	Tráfico de gestión de los dispositivos de la red
VLAN 40	Red Transito Internet	Tráfico de tránsito entre el firewall y el router
VLAN 50	Red de Videoconferencia	Tráfico de equipamiento de videoconferencia
VLAN 60	Red de Multifunción	Tráfico de equipos multifunción
VLAN 70	Red Transito usuarios	Tráfico de tránsito entre los switches de distribución/core y los firewalls

Tabla 11. Listado de VLANs configuradas en los firewalls

Atendiendo al volumen de tráfico esperado por cada VLAN, podemos considerar la siguiente distribución de VLANs por subinterfaz, teniendo en cuenta un firewall de 4 interfaces:

eth0	eth1	eth2	eth3
VLAN 60 VLAN 70	VLAN 20 VLAN 21 VLAN 22	VLAN 30 VLAN 40 VLAN 50	*SYNC*

Figura 32 Asignación de VLANs a Interfaces del firewall

La interfaz denotada como SYNC será la empleada para la sincronización entre el firewall activo y el pasivo según la configuración en alta disponibilidad, enviando la información necesaria para mantener la continuidad del servicio en caso de caída del firewall principal.

4.4.1.1 Alternativa de diseño

Una alternativa al diseño que se ha desarrollado en el apartado anterior, consistiría en separar el tráfico de cada una de las subredes de planta con el objetivo de poder aplicar políticas de seguridad distintas para cada uno de estos tráficos. Esta alternativa podría ser de utilidad si dentro de nuestro centro de coworking se quisiera separar de forma permanente a usuarios de diferentes sectores profesionales por planta, limitando el acceso entre plantas sólo a aquellas plantas destinadas a un mismo ámbito profesional.

Según este escenario, nuestro diseño lógico respondería al diagrama que se muestra a continuación en la figura 33:

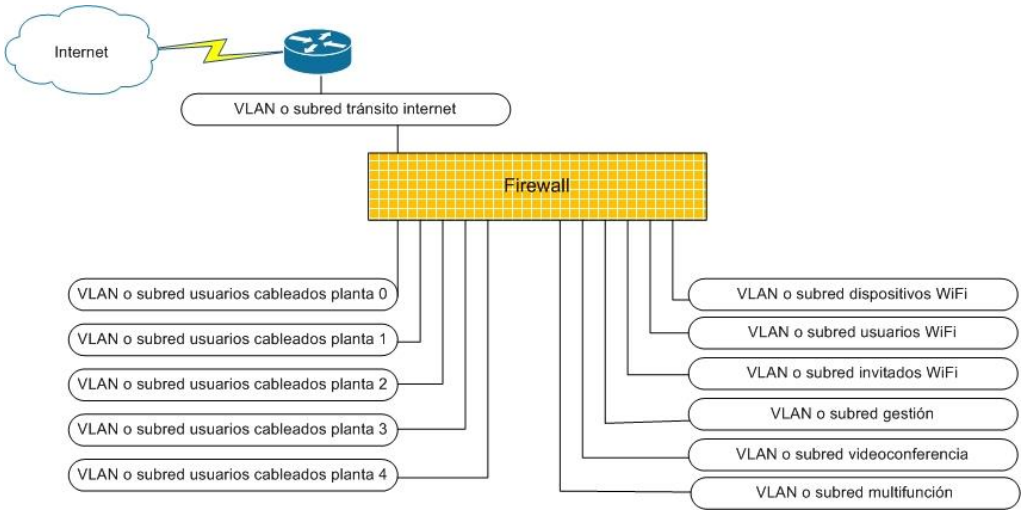


Figura 33. Alternativa de Diseño

Como puede observarse en la imagen, todo el tráfico entre plantas atraviesa el firewall, permitiendo que se apliquen políticas de seguridad y mecanismos de filtrado específicos para el tráfico de cada planta. Según este diseño, el único dispositivo encargado del nivel 3 o enrutamiento entre subredes será el firewall, tanto para el tráfico proveniente de las subredes de planta como para el tráfico del resto de subredes.

4.4.2 Plan de direccionamiento IP

En este bloque vamos a realizar la asignación de direcciones IP para cada una de las subredes de nuestra red.

Asignamos a nuestra red la dirección privada **192.168.0.0/20**. El prefijo de red o máscara nos indica que tenemos **disponibles 4.094 direcciones.**

En primer lugar definimos el número de direcciones IP necesarias para cada subred teniendo en cuenta las siguientes consideraciones:

- El número de direcciones necesarias para cada subred de usuarios de planta, se define teniendo en cuenta los datos de volumen de usuarios facilitados en el apartado caso de estudio.
- En el caso de las subredes de usuarios e invitados WiFi, se ha estimado el número de direcciones necesarias según el volumen de clientes WiFi esperados.
- Para las subred de dispositivos WiFi se ha considerado el total del equipamiento WiFi descrito en el apartado de equipamiento (27 puntos de acceso y 2 controladores)
- Para la subred de videoconferencia se consideran las dos direcciones para los dos equipos de videoconferencia.
- Para la subred de multifunción se consideran una dirección para cada uno de los equipos multifunción de planta.
- En el caso de la subred de gestión, son necesarias tantas direcciones como equipos de red gestionables.
- Para los firewalls, es necesaria una dirección por cada interfaz o subinterfaz, más una dirección VIP para cada interfaz o subinterfaz del firewall activo.
- Por último, necesitamos reservar dos direcciones IP adicionales que no están reflejadas dentro de ninguna VLAN. Se trata de las direcciones IP para la sincronización entre los dos firewalls.

Atendiendo a estas consideraciones la Tabla 12 resumen el número de direcciones necesarias para cada subred:

Subred	Nº Direcciones IP
Usuarios Planta 0	159
Usuarios Planta 1	172
Usuarios Planta 2	188
Usuarios Planta 3	188
Usuarios Planta 4	123
Usuarios WiFi	1000
Invitados WiFi	500
Dispositivos WiFi	32
Videoconferencia	5
Multifunción	8
Gestión	11
Transito Internet	4
Transito Usuarios	4
Sincronización FWs	2
TOTAL	2396

Tabla 12. Direcciones IP necesarias

A continuación se muestra el plan de direccionamiento resultante:

	Nº Direcciones IP	Bits Host	Nº Direcciones asignables	Máscara	Dirección de Subred	Primera dirección	Última dirección	Dirección de Broadcast
Usuarios WiFi	1000	10	1022	/22	192.168.0.0	192.168.0.1	192.168.3.254	192.168.3.255
Invitados WiFi	500	9	510	/23	192.168.4.0	192.168.4.1	192.168.5.254	192.168.5.255
Usuarios Planta 2	188	8	254	/24	192.168.6.0	192.168.6.1	192.168.6.254	192.168.6.255
Usuarios Planta 3	188	8	254	/24	192.168.7.0	192.168.7.1	192.168.7.254	192.168.7.255
Usuarios Planta 1	172	8	254	/24	192.168.8.0	192.168.8.1	192.168.8.254	192.168.8.255
Usuarios Planta 0	159	8	254	/24	192.168.9.0	192.168.9.1	192.168.9.254	192.168.9.255
Usuarios Planta 4	123	8	254	/24	192.168.10.0	192.168.10.1	192.168.10.254	192.168.10.255
Dispositivos WiFi	32	6	62	/26	192.168.11.0	192.168.11.1	192.168.11.62	192.168.11.63
Gestión	11	5	30	/27	192.168.11.64	192.168.11.65	192.168.11.94	192.168.11.95
Multifunción	8	4	14	/28	192.168.11.96	192.168.11.97	192.168.11.110	192.168.11.111
Videoconferencia	5	3	6	/29	192.168.11.112	192.168.11.113	192.168.11.118	192.168.11.119
Transito Internet	4	3	6	/29	192.168.11.120	192.168.11.121	192.168.11.126	192.168.11.127
Transito usuarios	4	3	6	/29	192.168.11.128	192.168.11.129	192.168.11.134	192.168.11.135
Sincronización FWs	2	3	6	/29	192.168.11.136	192.168.11.137	192.168.11.142	192.168.11.143

Tabla 13. Tabla de asignación de direcciones de subred.

Una vez que se ha definido el plan de direccionamiento IP de nuestra red, vamos a completar nuestro diagrama lógico añadiendo las direcciones IP asignadas a cada subred para tener toda la información del diseño lógico de nuestra red agrupada en un mismo diagrama.

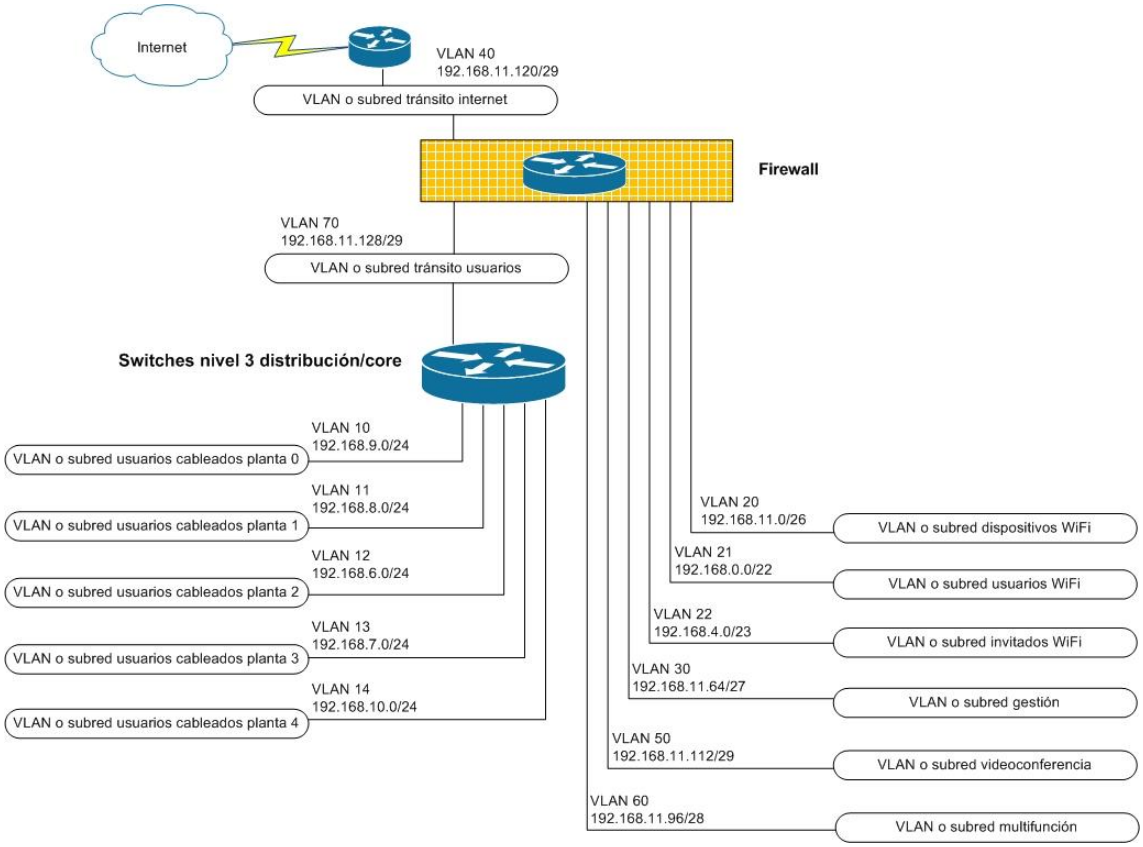


Figura 34. Diagrama lógico final.

4.5 Diseño físico

El diseño físico incluye todos los aspectos relativos a las conexiones físicas entre los dispositivos de nuestra red (interfaces de conexión en cada dispositivo, tipo de enlace, velocidad del puerto o interfaz, etc).

4.5.1 Tablas de Conexiones

En este apartado se detallan todas las tablas de conexiones físicas de cada dispositivo de nuestra red.

Para poder interpretar correctamente las tablas de conexiones de cada dispositivo primero se debe conocer la nomenclatura empleada para denotar a cada dispositivo así como la empleada para denotar a cada interfaz del mismo en función del tipo de dispositivo del que se trate.

- ***Nomenclatura del dispositivo: HostName***

  Para denotar a un dispositivo utilizamos el parámetro conocido como HostName. Se trata de un parámetro de la configuración inicial de cualquier dispositivo que nos sirve para identificarlo de forma única. Se suele establecer agrupando una serie de caracteres que nos indiquen características que identifiquen al dispositivo, como su ubicación, el tipo de dispositivo y un número. Como ejemplo, para establecer el HostName de uno de los firewalls de nuestro diseño empleamos el siguiente: CCMADFW01 (CC, centro de coworking; MAD, Madrid; FW, firewall; 01, número 1).

- ***Nomenclatura de interfaces switch***

  La nomenclatura empleada para denotar a una interfaz concreta de un switch es la siguiente: G1/0/10, donde
  - G indica que el puerto opera bajo el estándar GigaBitEthernet, por el cual sabemos que la velocidad del puerto será de 1 Gigabit por segundo.
  - 1, indica la posición del switch en el stack, en este caso se trata del primer switch del stack.
  - 0, indica que vamos a configurar los puertos que están integrados en la placa base. Si este valor es distinto de 0, indica que vamos a configurar puertos no integrados en la placa base (por ejemplo puertos de uplink o de cualquier modulo de puertos que se añada al switch)
  - 10, es el número de puerto dentro del switch.

- ***Nomenclatura de interfaces router***

  En el caso de los routers la nomenclatura empleada es prácticamente la misma que en los switches a excepción de que no se considera el primer número que indica la posición dentro del stack, ya que los routers no son dispositivos apilables. Se considera por lo tanto: G0/1, donde
  - G indica que el puerto opera bajo el estándar GigaBitEthernet, por el cual sabemos que la velocidad del puerto será de 1 Gigabit por segundo.
  - 0, indica que vamos a configurar los puertos que están integrados en la placa base. Si este valor es distinto de 0, indica que vamos a configurar puertos no integrados en la placa base (por ejemplo puertos de uplink o de cualquier modulo de puertos que se añada al router)

- 1, es el numero de puerto dentro del router.

Esta nomenclatura será la empleada también para los Controladores Inalámbrica, los puntos de acceso y los equipos de videoconferencia

- ***Nomenclatura de interfaces firewall***
  Para los firewalls emplearemos la nomenclatura: eth*X*, donde *X* será la posición de la interfaz. De esta forma tendremos las interfaces: eth0, eth1, eth2 y eth3.

4.5.1.1 Tabla de conexiones de firewalls

Los firewalls principal y secundario (CCMADFW01 y CCMADFW02) están conectados a los switches de distribución/core (CCMADSWDST) mediante tres enlaces a 1GBps por cada firewall, y entre sí mediante la interfaz de sincronización, el detalle de las interfaces empleadas para estos enlaces se indica a continuación:

Origen		Destino		Medio	Velocidad
Hostname	**Interface**	**Hostname**	**Interface**		
CCMADFW01	eth0	CCMADSWDST	G1/0/11	cobre	1Gb
CCMADFW01	eth1	CCMADSWDST	G1/0/13	cobre	1Gb
CCMADFW01	eth2	CCMADSWDST	G1/0/15	cobre	1Gb
CCMADFW01	eth3	CCMADFW02	eth3	cobre	1Gb
CCMADFW02	eth0	CCMADSWDST	G2/0/11	cobre	1Gb
CCMADFW02	eth1	CCMADSWDST	G2/0/13	cobre	1Gb
CCMADFW02	eth2	CCMADSWDST	G2/0/15	cobre	1Gb
CCMADFW02	eth3	CCMADFW01	eth3	cobre	1Gb

Tabla 14. Tabla de Conexiones de firewalls.

4.5.1.2 Tabla de conexiones de router

Los routers de salida a internet (CCMADRT01 y CCMADRT02) están conectados a los switches de distribución/core (CCMADSWDST) mediante enlaces de cobre a 1Gbps:

Origen		Destino		Medio	Velocidad
Hostname	**Interface**	**Hostname**	**Interface**		
CCMADRT01	G0/0	CCMADSWDST	G1/0/1	cobre	1Gb
CCMADRT02	G0/0	CCMADSWDST	G2/0/17	cobre	1Gb

Tabla 15. Tabla de conexiones de routers

4.5.1.3 Tabla de conexiones de controladores WiFi

Los controladores WiFi (CCMADWLC01 y CCMADWLC02) están conectados a los switches de distribución/core (CCMADSWDST) mediante dos enlaces de cobre por cada controlador a 1Gbps. El motivo por el que se utilizan dos enlaces, es porque los controladores cuentan con una interfaz dedicada a la gestión, de esta forma se tendrá un enlace para gestión y otro para el resto del tráfico. El detalle de interfaces empleadas y tipo de enlace se indica a continuación:

Origen		Destino		Medio	Velocidad
Hostname	**Interface**	**Hostname**	**Interface**		
CCMADWLC01	G0/0	CCMADSWDST	G1/0/3	cobre	1Gb
CCMADWLC01	G0/1	CCMADSWDST	G1/0/5	cobre	1Gb
CCMADWLC02	G0/0	CCMADSWDST	G2/0/3	cobre	1Gb
CCMADWLC02	G0/1	CCMADSWDST	G2/0/5	cobre	1Gb

Tabla 16. Tabla de Conexiones de Controladores Inalámbrica.

4.5.1.4 Tabla de conexiones switches distribución/core

Los switches de distribución/core (CCMADSWDST) están conectados a los routers (CCMADRT01 y CCMADRT02), a los controladores (CCMADWLC01 y CCMADWLC02) y a los firewalls (CCMADFW01 y CCMADFW02) mediante enlaces de cobre a 1 Gbps, y a los stack de los switches de planta (CCMADSWPL00, CCMADSWPL01, CCMADSWPL02, CCMADSWPL03 y CCMADSWPL04) mediante enlaces de fibra óptica multi-modo a 10Gbps. A continuación se detalla el tipo y número de enlaces para cada una de estas conexiones, así como las interfaces concretas empleadas para ello:

Origen		Destino		Medio	Velocidad
Hostname	**Interface**	**Hostname**	**Interface**		
CCMADSWDST	G1/0/1	CCMADRT01	G0/0	cobre	1Gb
CCMADSWDST	G1/0/3	CCMADWLC01	G0/0	cobre	1Gb
CCMADSWDST	G1/0/5	CCMADWLC01	G0/1	cobre	1Gb
CCMADSWDST	G1/0/11	CCMADFW01	eth0	cobre	1Gb
CCMADSWDST	G1/0/13	CCMADFW01	eth1	cobre	1Gb
CCMADSWDST	G1/0/15	CCMADFW01	eth2	cobre	1Gb
CCMADSWDST	G1/0/2	CCMADSWPL00	G1/1/1	Fibra MM	10Gb
CCMADSWDST	G1/0/4	CCMADSWPL01	G1/1/1	Fibra MM	10Gb
CCMADSWDST	G1/0/6	CCMADSWPL02	G1/1/1	Fibra MM	10Gb
CCMADSWDST	G1/0/8	CCMADSWPL03	G1/1/1	Fibra MM	10Gb
CCMADSWDST	G1/0/10	CCMADSWPL04	G1/1/1	Fibra MM	10Gb
CCMADSWDST	G2/0/17	CCMADRT02	G0/0	cobre	1Gb

CCMADSWDST	G2/0/3	CCMADWLC02	G0/0	cobre	1Gb
CCMADSWDST	G2/0/5	CCMADWLC02	G0/1	cobre	1Gb
CCMADSWDST	G2/0/11	CCMADFW01	eth0	cobre	1Gb
CCMADSWDST	G2/0/13	CCMADFW01	eth1	cobre	1Gb
CCMADSWDST	G2/0/15	CCMADFW01	eth2	cobre	1Gb
CCMADSWDST	G2/0/2	CCMADSWPL00	G4/1/1	Fibra MM	10Gb
CCMADSWDST	G2/0/4	CCMADSWPL01	G4/1/1	Fibra MM	10Gb
CCMADSWDST	G2/0/6	CCMADSWPL02	G5/1/1	Fibra MM	10Gb
CCMADSWDST	G2/0/8	CCMADSWPL03	G5/1/1	Fibra MM	10Gb
CCMADSWDST	G2/0/10	CCMADSWPL04	G3/1/1	Fibra MM	10Gb

Tabla 17. Tabla de Conexiones de Switches de Distribución.

4.5.1.5 Tabla de conexiones de switches de acceso

Los switches de acceso (CCMADSWPL00, CCMADSWPL01, CCMADSWPL02, CCMADSWPL03 y CCMADSWPL04) están conectados a los switches de distribución/core (CCMADSWDST) mediante enlaces de fibra óptica multi-modo a 10Gbps como ya vimos en la tabla de conexiones de estos últimos. Además, los switches de las planta están conectados a los puntos de acceso (CCMADAP0*X*PL00) que se distribuyen por cada planta con enlaces de cobre a 1Gbps. Por último, los switches de las plantas 0 y 1, se conectan también con los equipos de videoconferencia (CCMADVC00 y CCMADVC01) situados en dichas plantas, y con los equipos de multifunción situados uno por planta (CCMAMF0*X*).

A continuación se muestra el detalle de estas conexiones:

Origen		**Destino**		**Medio**	**Velocidad**
Hostname	**Interface**	**Hostname**	**Interface**		
CCMADSWPL00	G1/1/1	CCMADSWDST	G1/0/2	Fibra MM	10Gb
CCMADSWPL00	G4/1/1	CCMADSWDST	G2/0/2	Fibra MM	10Gb
CCMADSWPL00	G1/0/10	CCMADAP01PL00	G0/0	cobre	1Gb
CCMADSWPL00	G2/0/10	CCMADAP02PL00	G0/0	cobre	1Gb
CCMADSWPL00	G3/0/10	CCMADAP03PL00	G0/0	cobre	1Gb
CCMADSWPL00	G4/0/10	CCMADAP04PL00	G0/0	cobre	1Gb
CCMADSWPL00	G4/0/12	CCMADAP05PL00	G0/0	cobre	1Gb
CCMADSWPL00	G4/0/14	CCMADAP06PL00	G0/0	cobre	1Gb
CCMADSWPL00	G4/0/16	CCMADVC00	G0/0	cobre	1Gb
CCMADSWPL00	G4/0/18	CCMAMF00	G0/0	cobre	1Gb
CCMADSWPL01	G1/1/1	CCMADSWDST	G1/0/4	Fibra MM	10Gb
CCMADSWPL01	G4/1/1	CCMADSWDST	G2/0/4	Fibra MM	10Gb
CCMADSWPL01	G1/0/10	CCMADAP01PL01	G0/0	cobre	1Gb
CCMADSWPL01	G2/0/10	CCMADAP02PL01	G0/0	cobre	1Gb
CCMADSWPL01	G3/0/10	CCMADAP03PL01	G0/0	cobre	1Gb

CCMADSWPL01	G4/0/10	CCMADAP04PL01	G0/0	cobre	1Gb
CCMADSWPL01	G4/0/12	CCMADAP05PL01	G0/0	cobre	1Gb
CCMADSWPL01	G4/0/14	CCMADAP06PL01	G0/0	cobre	1Gb
CCMADSWPL01	G4/0/16	CCMADVC01	G0/0	cobre	1Gb
CCMADSWPL01	G4/0/18	CCMAMF01	G0/0	cobre	1Gb
CCMADSWPL02	G1/1/1	CCMADSWDST	G1/0/6	Fibra MM	10Gb
CCMADSWPL02	G5/1/1	CCMADSWDST	G2/0/6	Fibra MM	10Gb
CCMADSWPL02	G3/0/10	CCMADAP01PL02	G0/0	cobre	1Gb
CCMADSWPL02	G4/0/10	CCMADAP02PL02	G0/0	cobre	1Gb
CCMADSWPL02	G5/0/10	CCMADAP03PL02	G0/0	cobre	1Gb
CCMADSWPL02	G5/0/12	CCMADAP04PL02	G0/0	cobre	1Gb
CCMADSWPL02	G5/0/14	CCMADAP05PL02	G0/0	cobre	1Gb
CCMADSWPL02	G4/0/16	CCMAMF02	G0/0	cobre	1Gb
CCMADSWPL03	G1/1/1	CCMADSWDST	G1/0/8	Fibra MM	10Gb
CCMADSWPL03	G5/1/1	CCMADSWDST	G2/0/8	Fibra MM	10Gb
CCMADSWPL03	G3/0/10	CCMADAP01PL03	G0/0	cobre	1Gb
CCMADSWPL03	G4/0/10	CCMADAP02PL03	G0/0	cobre	1Gb
CCMADSWPL03	G4/0/10	CCMADAP03PL03	G0/0	cobre	1Gb
CCMADSWPL03	G5/0/12	CCMADAP04PL03	G0/0	cobre	1Gb
CCMADSWPL03	G4/0/14	CCMADAP05PL03	G0/0	cobre	1Gb
CCMADSWPL03	G4/0/16	CCMAMF03	G0/0	cobre	1Gb
CCMADSWPL04	G1/1/1	CCMADSWDST	G1/0/10	Fibra MM	10Gb
CCMADSWPL04	G3/1/1	CCMADSWDST	G2/0/10	Fibra MM	10Gb
CCMADSWPL04	G1/0/10	CCMADAP01PL04	G0/0	cobre	1Gb
CCMADSWPL04	G2/0/10	CCMADAP02PL04	G0/0	cobre	1Gb
CCMADSWPL04	G3/0/10	CCMADAP03PL04	G0/0	cobre	1Gb
CCMADSWPL04	G3/0/12	CCMADAP04PL04	G0/0	cobre	1Gb
CCMADSWPL04	G3/0/14	CCMADAP05PL04	G0/0	cobre	1Gb
CCMADSWPL04	G4/0/18	CCMAMF04	G0/0	cobre	1Gb

Tabla 18. Tabla de Conexiones de Switches de acceso

4.5.2 Diagrama físico

Una vez que se han detallado todas las conexiones entre todos los dispositivos de red, completamos nuestro diagrama físico, el cual nos muestra la arquitectura física completa de nuestra red:

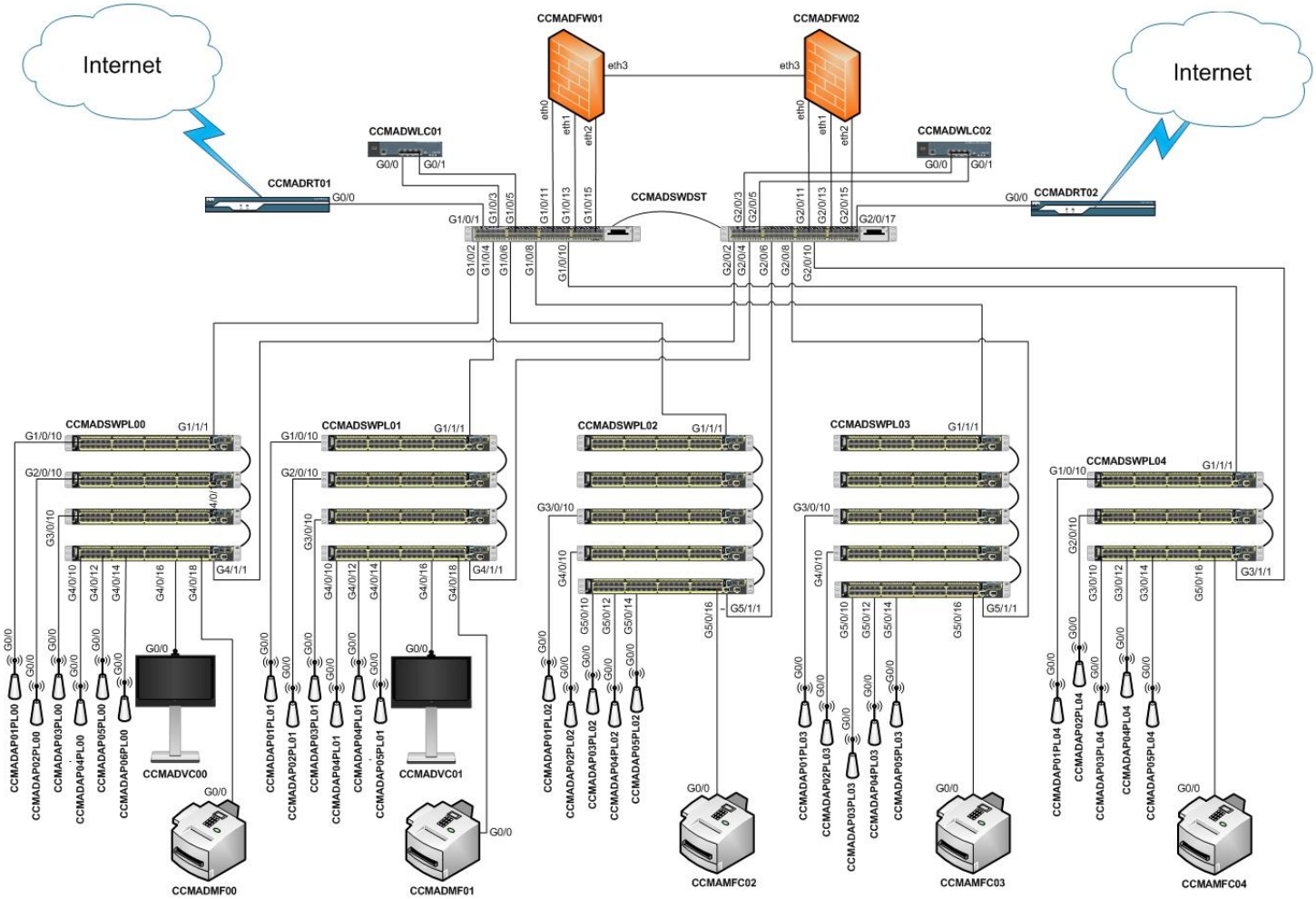


Figura 35. Diagrama físico.

4.6 Servicios de instalación

Los servicios de instalación comprenden el conjunto de tareas necesarias para llevar a cabo el despliegue físico y lógico de nuestra red. El objetivo de este apartado es definir cuáles son las tareas en las que se dividen los servicios de instalación necesarios para el despliegue de nuestra red y desarrollar la planificación de su ejecución en el tiempo.

4.6.1 Definición de tareas

Podemos definir el alcance de los servicios de instalación relativos al despliegue de nuestra red mediante las siguientes tareas:

1. **Análisis y diseño:** El primer paso para llevar a cabo el despliegue de nuestra red consiste en el análisis de la documentación relativa al proyecto, disponible como punto de partida, y el diseño de las fases de actuación para llevar a cabo el despliegue. En esta fase es habitual llevar a cabo reuniones con el cliente para poner en común cómo se ejecutará el proyecto, disponibilidades horarias, solicitudes o permisos de acceso al centro y/o cualquier otra aclaración que sea necesaria antes de comenzar.
    - Duración: 3 jornadas
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada.

2. **Pre-configuración del equipamiento**: Una vez que hemos terminado la fase de análisis y diseño, comenzamos con la configuración de cada dispositivo de red. Esta fase se puede desempeñar de forma previa a la instalación física del equipamiento en su ubicación final en las dependencias del cliente, habitualmente suele realizarse en un laboratorio de redes o cualquier sala destinada para este fin propiedad de la empresa encargada del despliegue.
    - Duración: 5 jornadas
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada

3. **Instalación física de todo el equipamiento**: Una vez que tenemos los equipos pre-configurados, procedemos a su instalación física en el centro de coworking teniendo en cuenta las condiciones definidas en el apartado de diseño físico.
    - Duración: 4 jornadas
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada

4. **Ajustes de configuración** Con todos los equipos correctamente instalados en sus ubicaciones finales, terminamos de realizar los ajustes de configuración que no hayan sido realizados de manera previa.
    - Duración: 2 jornadas
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada

5. **Pruebas de funcionamiento**: Una vez que todos los equipos estén instalados y configurados realizamos una serie de pruebas de funcionamiento para verificar que el funcionamiento de la red es el correcto.
    - Duración: 1 jornada
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada

6. **Puesta en marcha (Go-Live)**: Esta tarea se desempeña el día en el que la red va a estar a pleno funcionamiento o en su uso habitual para el cual se ha diseñado. En nuestro caso será el día en el que el centro de coworking abra sus puertas a empleados y clientes, por ello se requieren de tareas de monitorización y soporte ante posibles fallos que no hayan sido detectados en las fases previas.
    - Duración: 1 jornada
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada

7. **Documentación**: Una vez finalizado el despliegue es necesario documentar todos los aspectos de configuración que se han llevado a cabo para hacer entrega de los mismos al personal que vaya a estar al cargo de la administración de la red.
    - Duración: 3 jornadas
    - Esfuerzo: Perfil de Ingeniero, 8h/jornada

8. **Jefatura de Proyecto**: Es necesario contemplar dentro de los servicios de instalación la figura de un gestor o jefe del proyecto que se encargue de la coordinación del mismo.
    - Duración: 5 jornadas
    - Esfuerzo: Perfil de Jefe de Proyecto, 8h/jornada

Cualquier otro tipo de tarea que no haya sido especificada en el listado anterior (ej. tareas de cableado, albañilería, carpintería, etc), se asume que será llevada a cabo por otra entidad y por lo tanto queda excluida del alcance de los servicios de instalación incluidos en el proyecto.

La tabla 19 muestra el resumen de tareas y su duración:

Nº Perfiles	TAREA	DURACIÓN (jornadas)	ESFUERZO (h/jornadas)	TOTAL (horas)
Análisis y diseño				
1	Perfil de Ingeniero	3	8	24
Pre-configuración del equipamiento				
1	Perfil de Ingeniero	5	8	40
Instalación física del equipamiento				
2	Perfil de Técnico Instalador	4	8	64
Ajustes de configuración				
1	Perfil de Ingeniero	2	8	16
Pruebas de funcionamiento				
1	Perfil de Ingeniero	1	8	8
Puesta en marcha (Go-Live)				
1	Perfil de Ingeniero	1	8	8
Documentación				
1	Perfil de Ingeniero	3	8	24
Jefatura de proyecto				
1	Perfil de Jefe de Proyecto	5	8	40
TOTAL (horas) Servicios de Instalación				**224 horas**

Tabla 19. Servicios de Instalación: Resumen de Tareas

4.6.2 Planificación

El siguiente gráfico muestra la planificación en el tiempo de las tareas descritas en el apartado anterior:

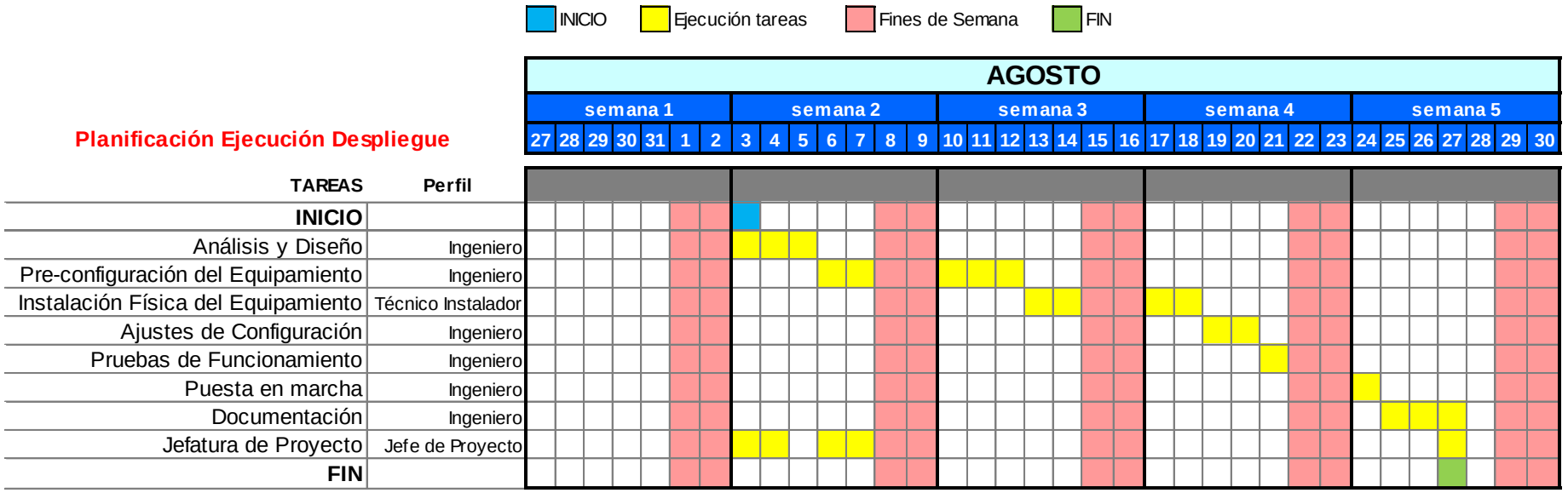


Figura 36. Planificación Ejecución Despliegue

4.7 Presupuesto económico

En este apartado se incluye el presupuesto económico total de la solución técnica desarrollada a lo largo de este bloque, en el presupuesto se incluyen los costes de todo el equipamiento de red, así como los costes totales de los servicios de instalación necesarios para el despliegue.

4.7.1 Costes del equipamiento

A continuación se detallan los costes totales de todo el equipamiento.

Equipamiento	Cant.	Coste unitario	Coste total
Switches de Nivel 2			
Switches Nivel 2, 48p de 1Gbps cobre + 2p de 10Gbps F.O MM	21	2.079,86 €	43.677,08 €
Módulos para Fibra Óptica MM a 10Gbps	10	218,34 €	2.183,35 €
Switches de Nivel 3			
Switches Nivel 3, 24p (necesario adapt. puerto)	2	10.845,51 €	21.691,08 €
Adaptador para Fibra Óptica MM 10Gbps	10	434,49 €	4.344,87 €
Adaptador para Cobre a 1Gbps	12	172,48 €	2.069,76 €
Firewalls			
Firewall con 4 interfaces cobre 1 Gbps	2	4.189, 85 €	8.379,70 €
Dispositivos red inalámbrica			
Controlador con licencias de base para 50 puntos de acceso (posibilidad de ampliación hasta 500 licencias)	2	10.916,76 €	21.833,52 €
puntos de acceso 802.11 ac. 5 GHz. Antenas Integradas	27	652,82 €	17.626,20 €
Equipamiento videoconferencia			
Equipo Videoconferencia con Pantalla de 55”, cámara zoom 4x, micrófonos de mesa y capacidad de videoconferencia múltiple y llamadas externas de hasta 4 participantes simultáneamente.	2	10.436,42 €	20.872,85 €
Equipamiento multifunción			
Equipo multifunción (impresora, fax y escáner)	5	2.286,90 €	11.434,50 €
TOTAL Coste equipamiento			**154.112,91 €**

Tabla 20. Presupuesto económico: Costes Equipamiento

4.7.2 Costes de los servicios de instalación

En la siguiente tabla se detallan los costes totales de los servicios de instalación:

Nº Perfiles	Tarea	Duración (jornadas)	Esfuerzo (h/jornadas)	TOTAL horas	Coste/h	Coste Total
Análisis y diseño de configuraciones						
1	Perfil Ingeniero	3	8	24	50 €	1.200 €
Pre-configuración del equipamiento						
1	Perfil Ingeniero	5	8	40	50 €	2.000 €
Instalación física de todo el equipamiento						
2	Perfil Técnico Instalador	4	8	64	40 €	2.560 €
Ajustes de Configuración						
1	Perfil Ingeniero	2	8	16	50 €	800 €
Pruebas de Funcionamiento						
1	Perfil Ingeniero	1	8	8	50 €	400 €
Puesta en Marcha (Go-Live)						
1	Perfil Ingeniero	1	8	8	50 €	400 €
Documentación						
1	Perfil Ingeniero	3	8	24	50 €	1.200 €
Jefatura de Proyecto						
1	Perfil Jefe de Proyecto	5	8	40	45 €	1.800 €
					TOTAL Coste Servicios de Instalación	**10.360,00€**

Tabla 21. Presupuesto económico: Costes Servicios de Instalación

4.7.3 Costes del proyecto

Total Coste Equipamiento	154.112,91 €
Total Coste Servicios de Instalación	10.360,00 €
TOTAL COSTE PROYECTO	**164.472,91 €**

En presupuesto total del Proyecto asciende a CIENTO SESENTA Y CUATRO MIL CUATROCIENTOS SETENTA Y DOS EUROS CON NOVENTA Y UNO CÉNTIMOS.

Fdo:

Irene Sánchez Blázquez.
Ingeniera Técnica de Telecomunicaciones.

Capítulo 5

Conclusiones

Con el desarrollo de este proyecto fin de carrera se ha pretendido afrontar de forma completa desde una fase de pre-venta, el desarrollo de un proyecto de telecomunicaciones basado en el despliegue de una red para un centro de coworking. Además de todo el desarrollo relativo a la definición de la solución técnica propuesta, se han incluido especificaciones de diseño a alto nivel, de las que se podría hacer uso en una fase de post-venta en caso de la ejecución real del proyecto.

Por lo tanto, todos los conocimientos aplicados en el presente proyecto son relativos a la ejecución de proyectos de telecomunicaciones en su fase de análisis, estudio, diseño y definición de la solución, fase previa a la venta (pre-venta), así como parte de las tareas aplicadas en la fase de ejecución, configuración y puesta en marcha del diseño, fase posterior a la venta (post-venta).

Los resultados de este desarrollo se han intentado exponer a través de la memoria en el mismo orden en el que han ido elaborados, con el objetivo de que el lector pueda entender con mayor facilidad los pasos que así se exponen y el sentido general de la solución propuesta y del proyecto fin de carrera que la engloba.

Los fundamentos teóricos para el desarrollo del proyecto se incluyen en los apartados del bloque de Estado del Arte, en el cual se resumen las bases teóricas de aquellos conceptos de mayor relevancia en el desarrollo del proyecto. Este apartado se ha entendido no como una bibliografía de fundamentos básicos, si no como un resumen del detalle de aquellos conceptos de mayor relevancia en la ejecución del proyecto.

La red resultante del desarrollo de este proyecto, cumple con las siguientes características:

- **Escalabilidad**: Se trata de una red fácilmente escalable debido a su arquitectura basada en capas con una capa de acceso dedicada a la conectividad directa con los

dispositivos de usuario, equipos de videoconferencia y puntos de acceso, y una capa de distribución/core dedicada al enrutamiento de nivel 3, procesamiento de paquetes y aplicación de políticas de seguridad. En caso de crecimiento, se pueden ir añadiendo nuevos switches a la capa de acceso que serán soportados por el resto de equipamiento ya existente en las capas superiores.

- **Alta disponibilidad (Redundancia)**: La red ofrece una configuración de alta disponibilidad en aquellos equipos más críticos, de tal forma que si se produce un fallo o caída en uno de ellos, la continuidad del servicio no se verá afectada.

- **Seguridad:** Además, la red resultante es una red segura ya que dispone de firewalls que controlan los flujo de tráfico que circulan por la red, aplicando reglas de seguridad y filtrado.

La elección del diseño y del equipamiento de la red se ha hecho considerando la mejor solución técnica en comparación con el precio. De esta forma, se ha evitado sobredimensionar la solución técnica propuesta a pesar de no disponer de un presupuesto limitado, con el fin de aproximar lo máximo posible el desarrollo de este proyecto a un caso real.

El alcance de los servicios de instalación incluidos, cubre todas las tareas de instalación y configuración de la red proporcionadas habitualmente por la empresa integradora de telecomunicaciones que ofrece la propuesta de solución técnica, sin ser un proyecto completo o “llave en mano” al no incluirse las tareas relacionadas con el despliegue de cableado necesario para la conectividad de los equipos.

Referencias

[1] ISO/IEC 27001:2013, “Information security management”, Octubre 2013. *http://www.iso.org/iso/es/home/standards/management-standards/iso27001.html*

[2] IEEE 802.1Q-2014, “Bridges and Bridged Networks”, Noviembre 2014. *http://www.ieee802.org/1/pages/802.1Q.html*

[3] RFC 4632 "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", Agosto 2006. https://tools.ietf.org/html/rfc4632. [Último acceso: Junio 2015]

[4] RFC 1878 “Variable Length Subnet Table For IPv4”, Diciembre 1995. ttps://tools.ietf.org/html/rfc1878 [Último acceso: Junio 2015]

[5] RFC 2663 “Terminología y consideraciones sobre Traducción de Direcciones IP”, Agosto 1999. http://www.rfc-es.org/rfc/rfc2663-es.txt [Último acceso: Junio 2015]

[6] L. Zhang “A Retrospective View of NAT” The IETF Journal, 2007 Vol. 3 Issue 2

[7] James F. Kurose. Keith W. Ross, “Computer Networking: a top-down approach,” Pearson, 6th edition. 2013.

[8] Wendell Odom “CCNA Routing and Switching 200-120 Official Cert Guide Library”, Cisco Press, 1st edition, Mayo 2013

[9] A. Woland, K. Redmon “CCNP Security SISAS 300-208 Official Cert Guide” Cisco Press, 1st edition, Mayo 2015.

[10] J. Geier “Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications, 2nd Edition” Cisco Press, 2th edition. Mayo 2015

[11] Matthew S. Gast “802.11 Wireless Networks: The Definitive Guide” 2nd edition O`Reilly, 2005

[12] Ekahau Site Survey http://www.ekahau.com/wifidesign/ekahau-site-survey. [Último acceso: Junio 2015]

[13]Cisco Video Conferencing Systems. http://www.cisco.com/c/en/us/products/conferencing/video-conferencing/index.html [Último acceso: Junio 2015]

Glosario de términos y acrónimos

CIDR	Classless Inter-Domain Routing
Coworking	(anglicismo) trabajo cooperativo
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
dBm	Decibelio-milivatio
GHz	Gigahercio
Gbit	Gigabit
Gbps	Gigabit por segundo
IEEE	Institute of Electric and Electronic Engineers
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization.
MAC	Media Access Control
MCU	Multipoint Control Unit
NAT	Network Address Translation
RFC	Requests for Comments
RSSI	Received Signal Strength Indicator
VIP	Virtual Internet Protocol
VLAN	Virtual Local Area Network
VLSM	Variable Lenght Subnet Mask
WiFi	Wireless Fidelity

Anexo I: Equipamiento

En este anexo se incluye el detalle del equipamiento real que se ha considerado para el diseño de la red del presente proyecto fin de carrera.

- ***Switches capa de acceso (nivel 2)***

Fabricante	Código de producto	Descripción	Cant.
Cisco	WS-C2960X-24PD-L	Switches Nivel 2, 48p de 1Gbps cobre + 2p de 10Gbps F.O MM	21

Figura 37. Switch WS-C2960X-24PD-L

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

- ***Switches capa distribución/core (nivel 3)***

Fabricante	Código de producto	Descripción	Cant.
Cisco	WS-C3850-24S	Switches Nivel 3, 24p (necesario adaptador puerto)	2

Figura 38. Switch WS-C3850-24S

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/data_sheet_c78-720918.html

Fabricante	Código de producto	Descripción	Cant.
Cisco	SFP-10G-SR=	Adaptador puerto para enlace Fibra Óptica MultiModo 10Gbps	10

Figura 39. Adaptador SFP-10G-SR=

Fabricante	Código de producto	Descripción	Cant.
Cisco	GLC-T=	Adaptador puerto para enlace de cobre a 1Gbps	12

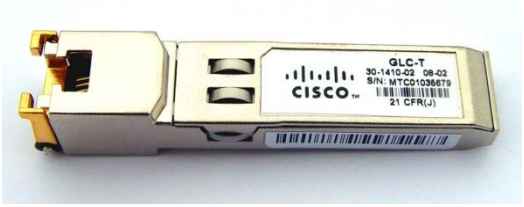


Figura 40. Adaptador GLC-T=

http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html

- ***Firewalls***

Fabricante	Código de producto	Descripción	Cant.
Checkpoint	CPAP-SG4400-NGFW	4400 Next-Gen Firewall	2

Figura 41. Firewall CPAP-SG4400-NGFW

http://www.checkpoint.com/downloads/product-related/datasheets/4400-appliance-datasheet.pdf

- ***Puntos de acceso y controladores***

Fabricante	Código de producto	Descripción	Cant.
Cisco	AIR-CT5520-50-K9	Controlador WiFi con licencias de base para 50 Puntos de Acceso (posibilidad de ampliación hasta 500 licencias)	2

Figura 42. Controlador AIR-CT5520-50-K9

http://www.cisco.com/c/en/us/products/collateral/wireless/5520-wireless-controller/datasheet-c78-734257.pdf

Fabricante	Código de producto	Descripción	Cant.
Cisco	AIR-CAP3702I-E-K9	Puntos de Acceso 802.11 ac. 5 GHz. antenas Integradas	27

Figura 43. Punto de acceso AIR-CAP3702I-E-K9

http://www.cisco.com/c/en/us/products/collateral/wireless/3700-series-access-point/data_sheet_c78-729421.html

- ***Equipo de videoconferencia***

Fabricante	Código de producto	Descripción	Cant.
Cisco	CTS-MX300-K9	Equipo Videoconferencia con Pantalla de 55”, cámara zoom 4x, micrófonos de mesa y capacidad de videoconferencia múltiple y llamadas externas de hasta tres participantes simultáneamente.	2

http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/telepresence-mx-series/data-sheet-c78-729734.html

- ***Equipo multifunción***

Fabricante	Código de producto	Descripción	Cant.
OKI	OKI MC770DN	IMPRESORA MULTIFUNCION LASER COLOR OKI MC770DN FAX DUPLEX/RED	5

Figura 44. Multifunción OKI MC770DN

http://www.mastoner.com/images/pdfs/45376114.pdf

Anexo II: Planificación y presupuesto

En este anexo se incluye la planificación de las fases en las que se divide el desarrollo del presente proyecto fin de carrera así como el cálculo del coste total que supone la ejecución del mismo.

- ***Planificación***

La elaboración del proyecto supone una duración total de 140 días repartidos desde Enero hasta Mayo de 2015. Cada jornada de trabajo consta de 4 horas lo que hace un total de 560 horas dedicadas a la elaboración del proyecto teniendo en cuenta la realización de la memoria.

A continuación se exponen las fases en las que se divide el desarrollo del proyecto:

Fase 1. **Elaboración del caso de estudio:** La primera fase consiste en la elaboración del caso de estudio en el que se basa el desarrollo del proyecto, en esta fase se describen las características del centro de coworking, se crean todos los planos de planta del centro y se definen los requisitos de la red de telecomunicaciones a diseñar. (16 horas, 4 días)

Fase 2. **Análisis de los requisitos y documentación**: Después de definir de forma completa el caso de estudio, se analizan los requisitos que se exponen en el mismo, y se lleva a cabo una fase de documentación, con el fin de recopilar los fundamentos teóricos más importantes que nos ayuden a definir los objetivos técnicos derivados del caso de estudio y afrontar el planteamiento inicial de la solución técnica. (56 horas, 14 días)

Fase 3. **Definición de la solución técnica**: En esta fase se realiza el desarrollo de la solución técnica que responde a los requisitos expuestos en el caso de estudio. El desarrollo de la misma se puede dividir a su vez en las siguientes fases:

Fase 3.1. **Planteamiento inicial de diseño**: En esta fase se define el planteamiento inicial de la solución técnica que se irá desarrollando en los apartados siguientes. Como parte del planteamiento inicial se describe la división de nuestra red física en diferentes redes lógicas o VLANs. (16 horas, 4 días)

Fase 3.2. **Red cableada:** Después del planteamiento inicial de diseño, continuamos la solución técnica con la definición del diseño para la infraestructura de la red cableada. Se define la arquitectura física de la red cableada y el equipamiento necesario para llevar a cabo dicha arquitectura. También se definen ciertos aspectos de la arquitectura lógica como la configuración de varios clusters de alta disponibilidad para aquellos equipos más críticos. (80 horas, 20 días)

Fase 3.3. **Red inalámbrica:** Esta fase consiste en definir el diseño para la infraestructura de la red inalámbrica. Para ello, se realiza la simulación de un estudio de cobertura inalámbrica mediante el software Ekahau Site Survey, del cual se obtiene el equipamiento necesario para completar la infraestructura de la red inalámbrica de nuestro diseño. (80 horas, 20 días)

Fase 3.4. **Ampliación de detalles de diseño**: En esta fase se agrupan todos los detalles de diseño físico y lógico que se han ido describiendo hasta el momento en las fases anteriores y se completa el diseño, terminando de definir la arquitectura lógica completa de nuestra red. (100 horas, 25 días)

Fase 3.5. **Diseño físico:** Una vez que se ha completado el diseño lógico de nuestra red, en esta fase se termina de completar el diseño físico de la misma, para ello se agrupa toda la información de la arquitectura física de nuestra red que se ha ido definiendo en las fases anteriores, mediante un diagrama físico; y se detallan todas las conexiones físicas entre los dispositivos que forman nuestra red, mediante las tablas de conexiones. (36 horas, 9 días)

Fase 3.6. **Servicios de instalación:** En esta fase se define la planificación de los servicios de instalación para llevar a cabo el despliegue de la red que se ha diseñado. (8 horas, 2 días)

Fase 3.7. **Presupuesto económico:** La última fase de definición de la solución técnica consiste en elaborar el presupuesto económico total de la solución que se ha desarrollado. (8 horas, 2 días)

Fase 4. **Elaboración de la memoria**: Por último, se incluye una fase dedicada a la elaboración de la memoria. (160 horas, 40 días)

Todas estas fases y su duración en el tiempo se resumen en la tabla 22.

Nº FASE	DESCRIPCIÓN	Días	Horas/día	Total horas
1	Elaboración del caso de estudio	4	4	16
2	Análisis de los requisitos y documentación	14	4	56
3.1	Planteamiento inicial de diseño	4	4	16
3.2	Red cableada	20	4	80
3.3	Red inalámbrica	20	4	80
3.4	Ampliación de detalles de diseño	25	4	100
3.5	Diseño físico	9	4	36
3.6	Servicios de instalación	2	4	8
3.7	Presupuesto económico	2	4	8
4	Elaboración de la memoria	40	4	160
			TOTAL (Horas)	**560**

Tabla 22. Planificación proyecto fin de carrera

A continuación se refleja de forma gráfica la planificación en el tiempo por semana y mes de todas las fases descritas en el apartado anterior:

Figura 45. Planificación proyecto fin de carrera

- ***Presupuesto***

A continuación se indica el presupuesto económico para la elaboración del presente proyecto fin de carrera, el cual estará formado por el coste total de horas de trabajo empleadas en la elaboración del proyecto y los costes de los materiales empleados en el desarrollo del mismo.

En cuanto al coste total por horas de trabajo, se ha considerado un coste/hora de 35 euros, tal cual se detalla en la tabla 23.

Nº FASE	DESCRIPCIÓN	Total horas	Coste/hora	Total coste
1	Elaboración del caso de estudio	16	35,00 €	560,00 €
2	Análisis de los requisitos y documentación	56	35,00 €	1.960,00 €
3.1	Planteamiento inicial de diseño	16	35,00 €	560,00 €
3.2	Red cableada	80	35,00 €	2.800,00 €
3.3	Red inalámbrica	80	35,00 €	2.800,00 €
3.4	Ampliación de detalles de diseño	100	35,00 €	3.500,00 €
3.5	Diseño físico	36	35,00 €	1.260,00 €
3.6	Servicios de instalación	8	35,00 €	280,00 €
3.7	Presupuesto económico	8	35,00 €	280,00 €
4	Elaboración de la memoria	160	35,00 €	5.600,00 €
			TOTAL coste horas de trabajo	19.600,00 €

Tabla 23. Costes por horas de trabajo

Los costes de los materiales hardware y software empleados para el desarrollo del proyecto se detallan en la figura 46.

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor:	Irene Sánchez Blázquez
2.- Departamento:	Ing. Telecomunicaciones, esp.: sonido e imagen
3.- Descripción del Proyecto:	
- Titulo	**Diseño de una red de relecomunicaciones en un centro de coworking**
- Duración (meses)	5
- Tasa de costes Indirectos:	20%
4.- Presupuesto total del Proyecto (valores en Euros):	€ 22.384,00

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	Categoría	Dedicación (horas)	Coste/hora	Coste (Euro)
Irene Sánchez	Ingeniero	560	35,00	€ 19.600,00
			Total	€ 19.600,00

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
Ordenador Portátil gama media	€ 700,00	100	5	60	€ 58,33
Lic. Software Ekahau Site Survey	€ 250,00	100	1	60	€ 4,17
Lic. Software Microsoft Office	€ 150,00	100	5	60	€ 12,50
				Total	€ 75,00

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

6.- Resumen de costes

Costes totales	Total
Personal	€ 19.600,00
Amortización	€ 75,00
Subcontratación de tareas	€ -
Costes de funcionamiento	€ -
Costes Indirectos	€ 2.709,00
Total	€ 22.384,00

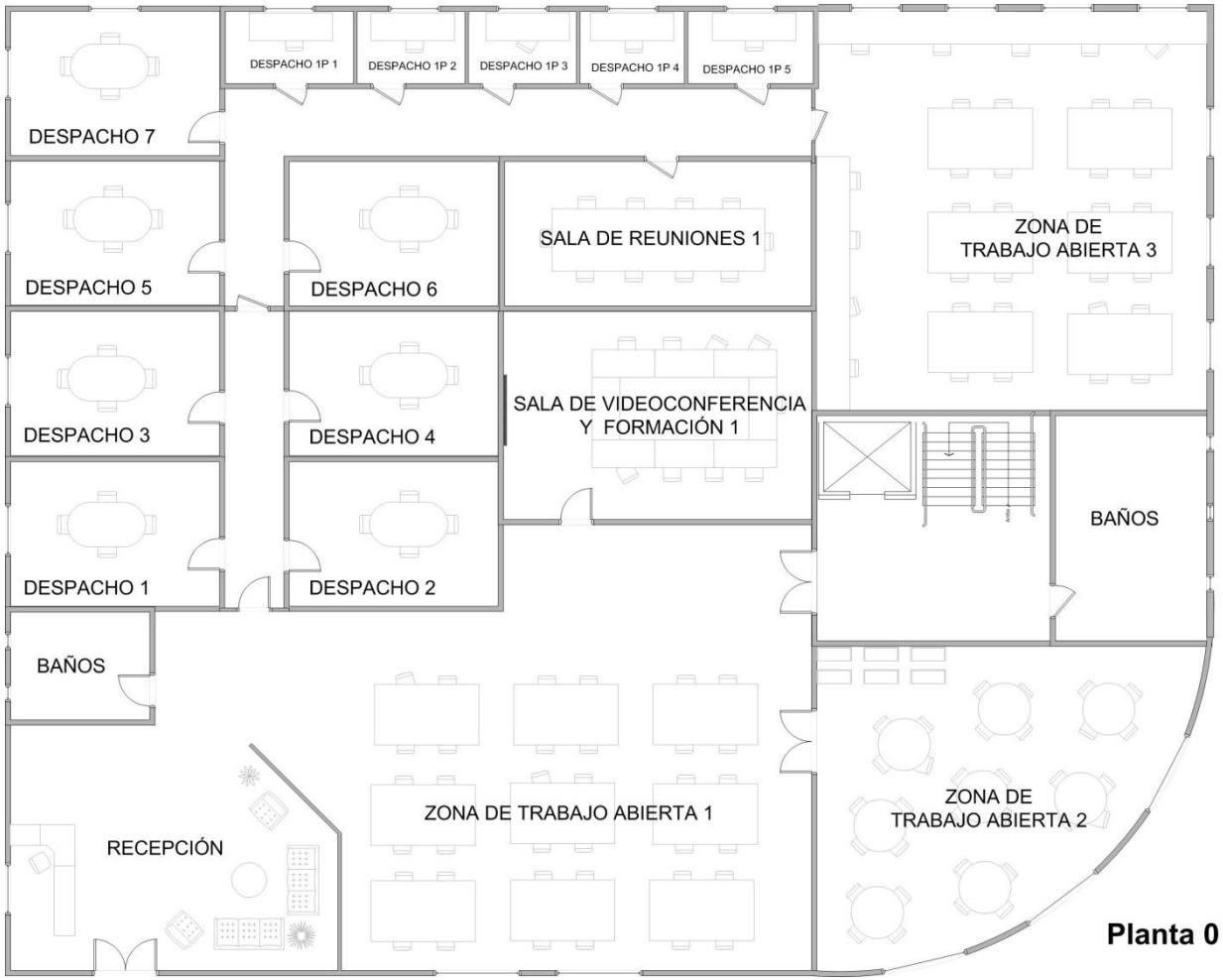
Figura 46. Presupuesto proyecto fin de carrera

El presupuesto total del Proyecto asciende a VEINTIDOS MIL TRESCIENTOS OCHENTA Y CUATRO EUROS.

Fdo:

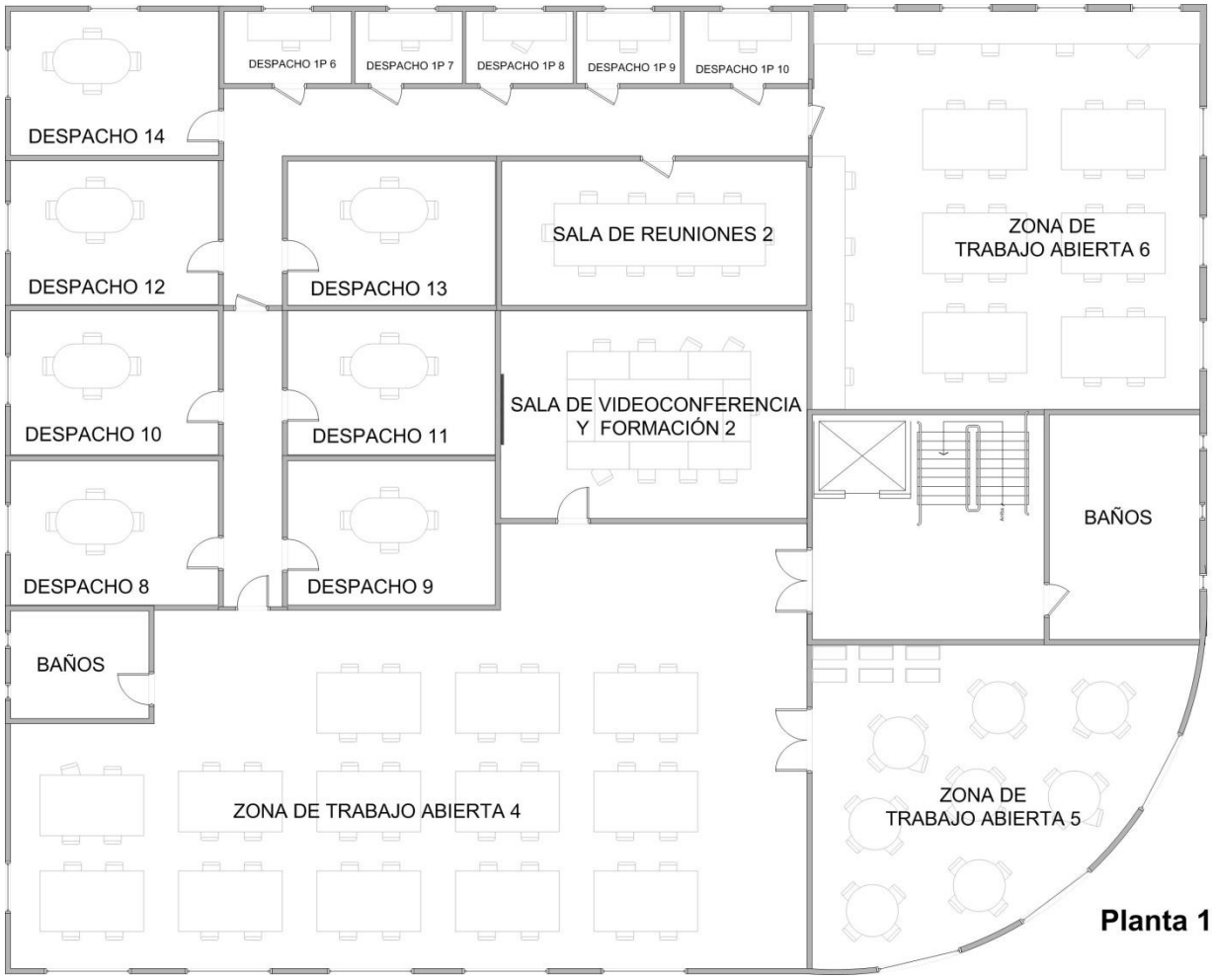
Irene Sánchez Blázquez.
Ingeniera Técnica de Telecomunicaciones

Anexo III: Planos de Planta



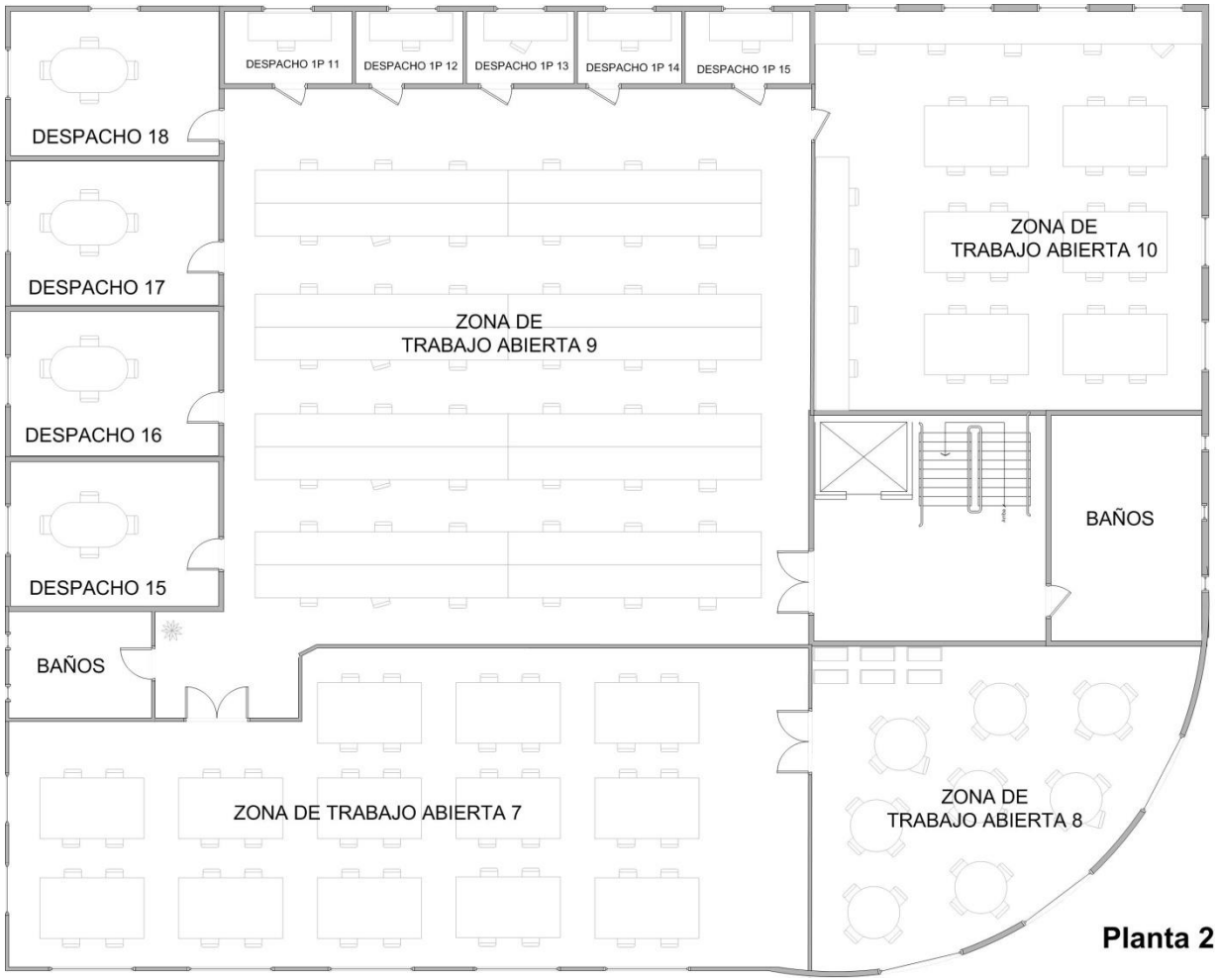
PLANTA 0	Cant.	Nº Puestos
Recepción	1	1
Baños	2	-
Zonas de Trabajo Abiertas	3	101
Despachos	7	28
Despachos 1P	5	5
Salas de Reuniones	1	10
Salas de Videoconferencia	1	9
Cocina /Comedor	-	-
Zona Exterior	-	-
TOTAL Nº PUESTOS DE TRABAJO		154

Figura 47. Plano de Planta: Planta 0



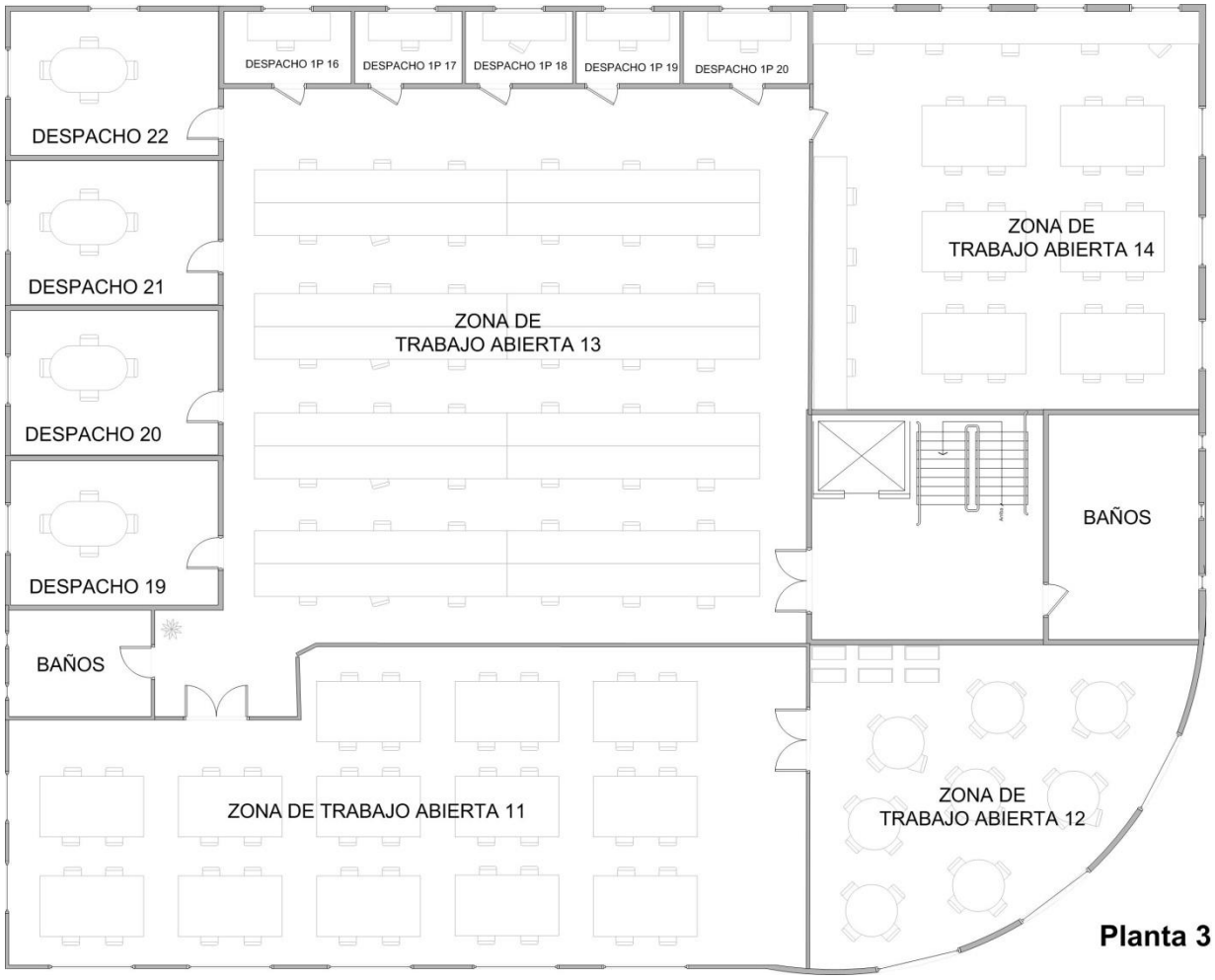
PLANTA 1	Cant.	Nº Puestos
Recepción	-	-
Baños	2	-
Zonas de Trabajo Abiertas	3	117
Despachos	7	28
Despachos 1P	5	5
Salas de Reuniones	1	10
Salas de Videoconferencia	1	9
Cocina /Comedor	-	-
Zona Exterior	-	-
TOTAL Nº PUESTOS DE TRABAJO		169

Figura 48. Plano de Planta: Planta 1



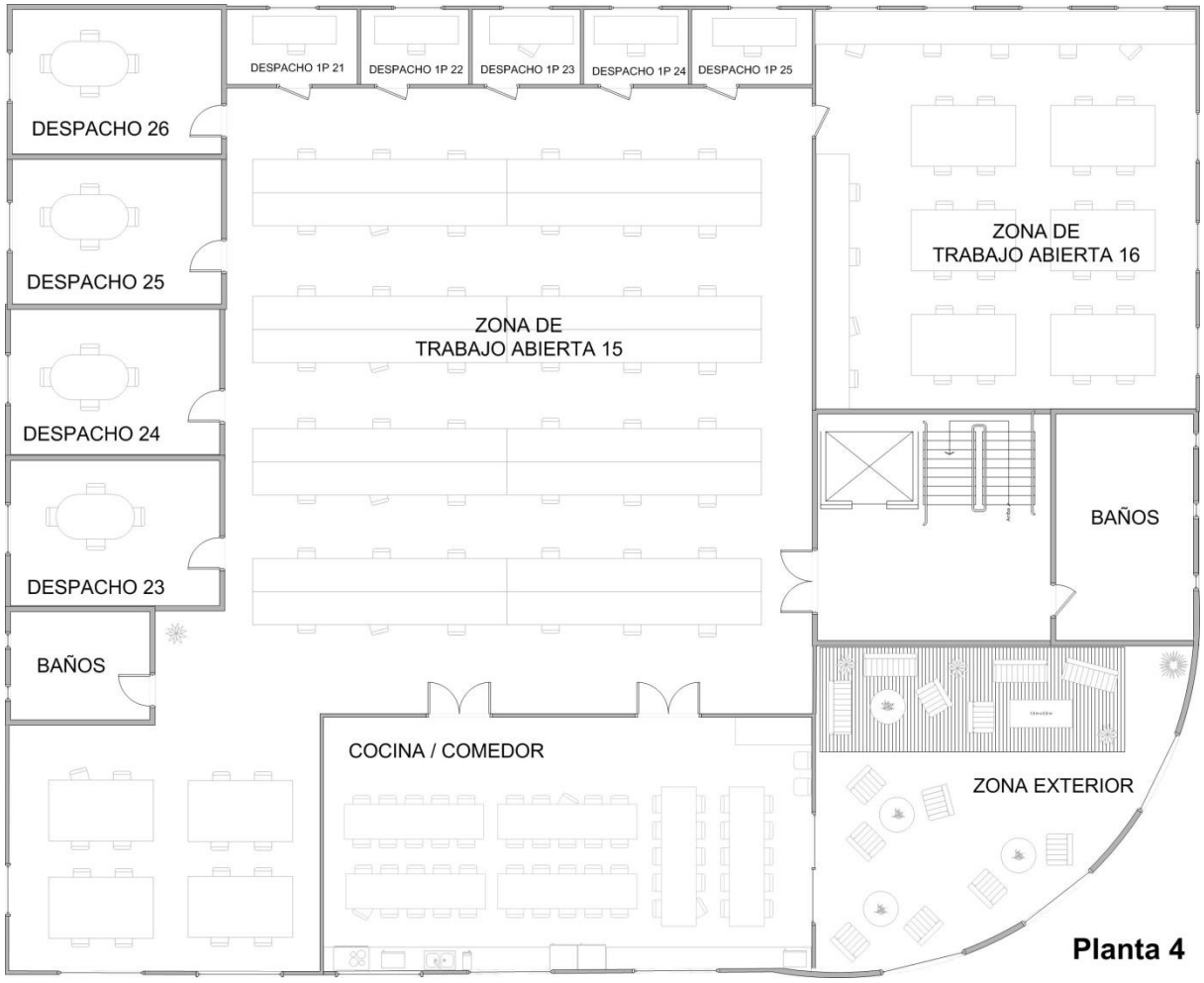
PLANTA 2	**Cant.**	**Nº Puestos**
Recepción	-	-
Baños	2	-
Zonas de Trabajo Abiertas	4	165
Despachos	4	16
Despachos 1P	5	5
Salas de Reuniones	-	-
Salas de Videoconferencia	-	-
Cocina /Comedor	-	-
Zona Exterior	-	-
TOTAL Nº PUESTOS DE TRABAJO		186

Figura 49. Plano de Planta: Planta 2



PLANTA 3	Cant.	Nº Puestos
Recepción	-	-
Baños	2	-
Zonas de Trabajo Abiertas	4	165
Despachos	4	16
Despachos 1P	5	5
Salas de Reuniones	-	
Salas de Videoconferencia	-	
Cocina /Comedor	-	-
Zona Exterior	-	-
TOTAL Nº PUESTOS DE TRABAJO		186

Figura 50. Plano de Planta: Planta 3



PLANTA 4	Cant.	Nº Puestos
Recepción	-	-
Baños	2	-
Zonas de Trabajo Abiertas	2	97
Despachos	4	16
Despachos 1P	5	5
Salas de Reuniones	-	-
Salas de Videoconferencia	-	-
Cocina /Comedor	1	-
Zona Exterior	1	-
TOTAL Nº PUESTOS DE TRABAJO		118

Figura 51. Plano de Planta: Planta 4